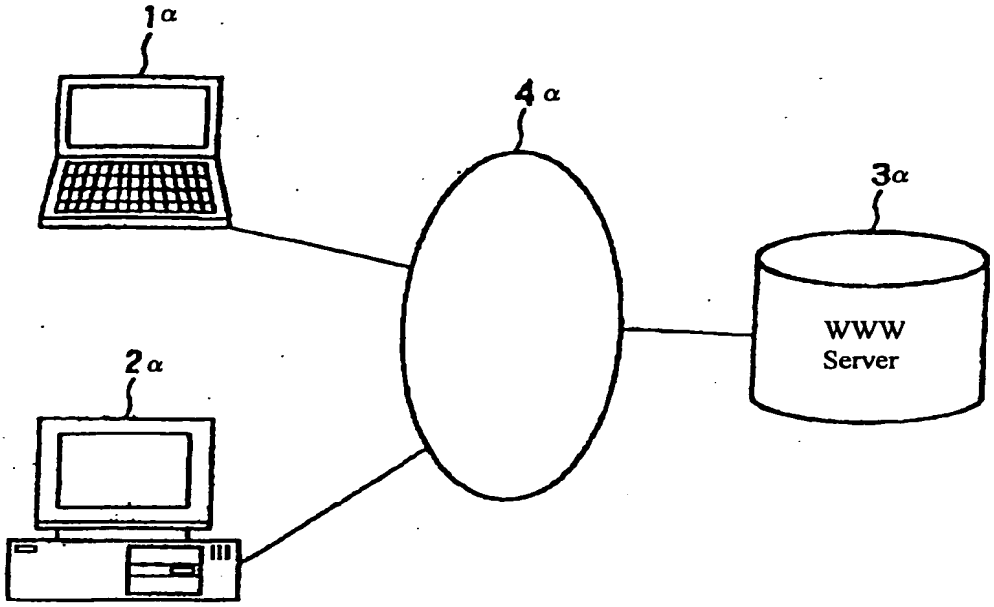
FIG.1



09700390 "09E00450

FIG.2

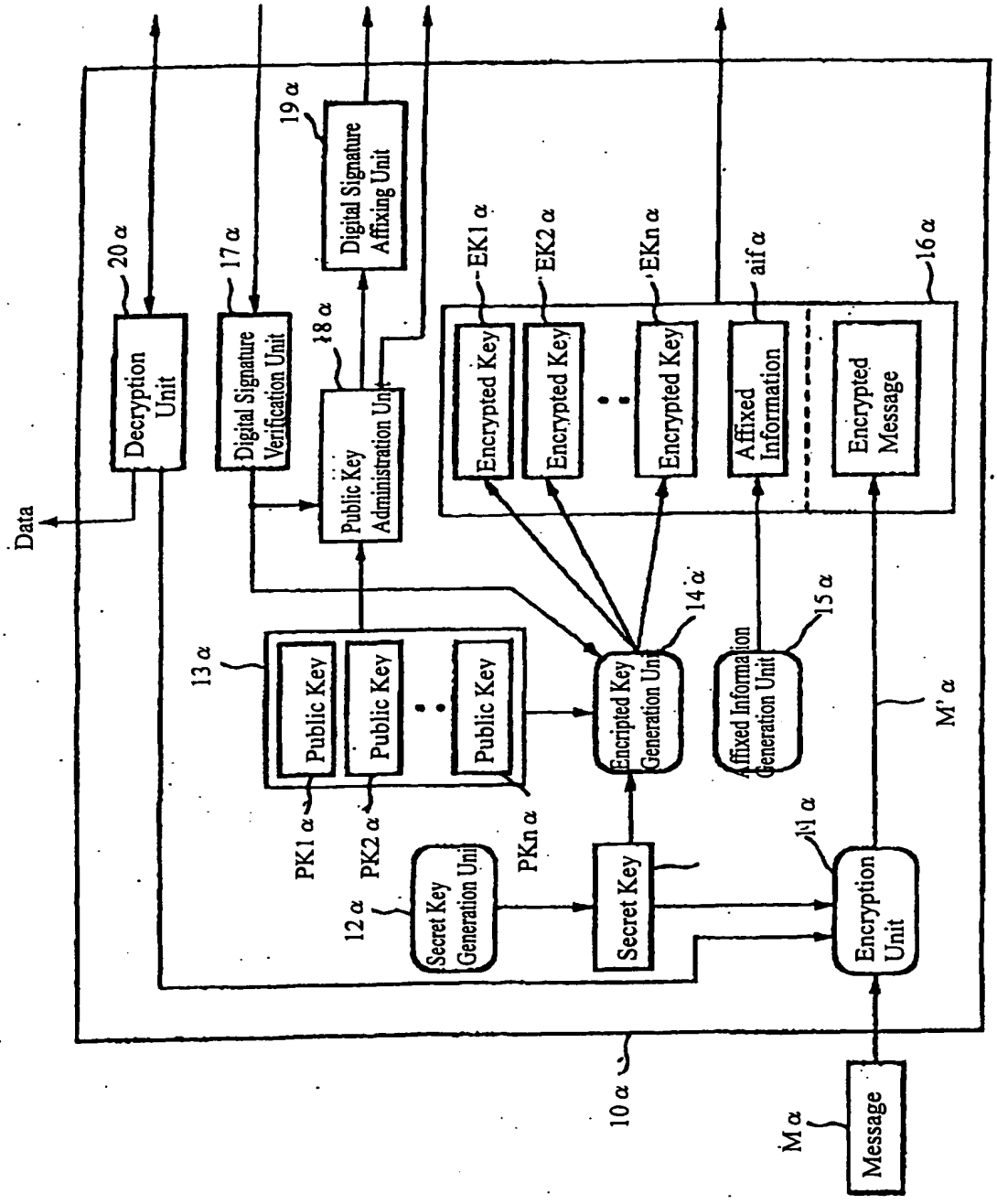
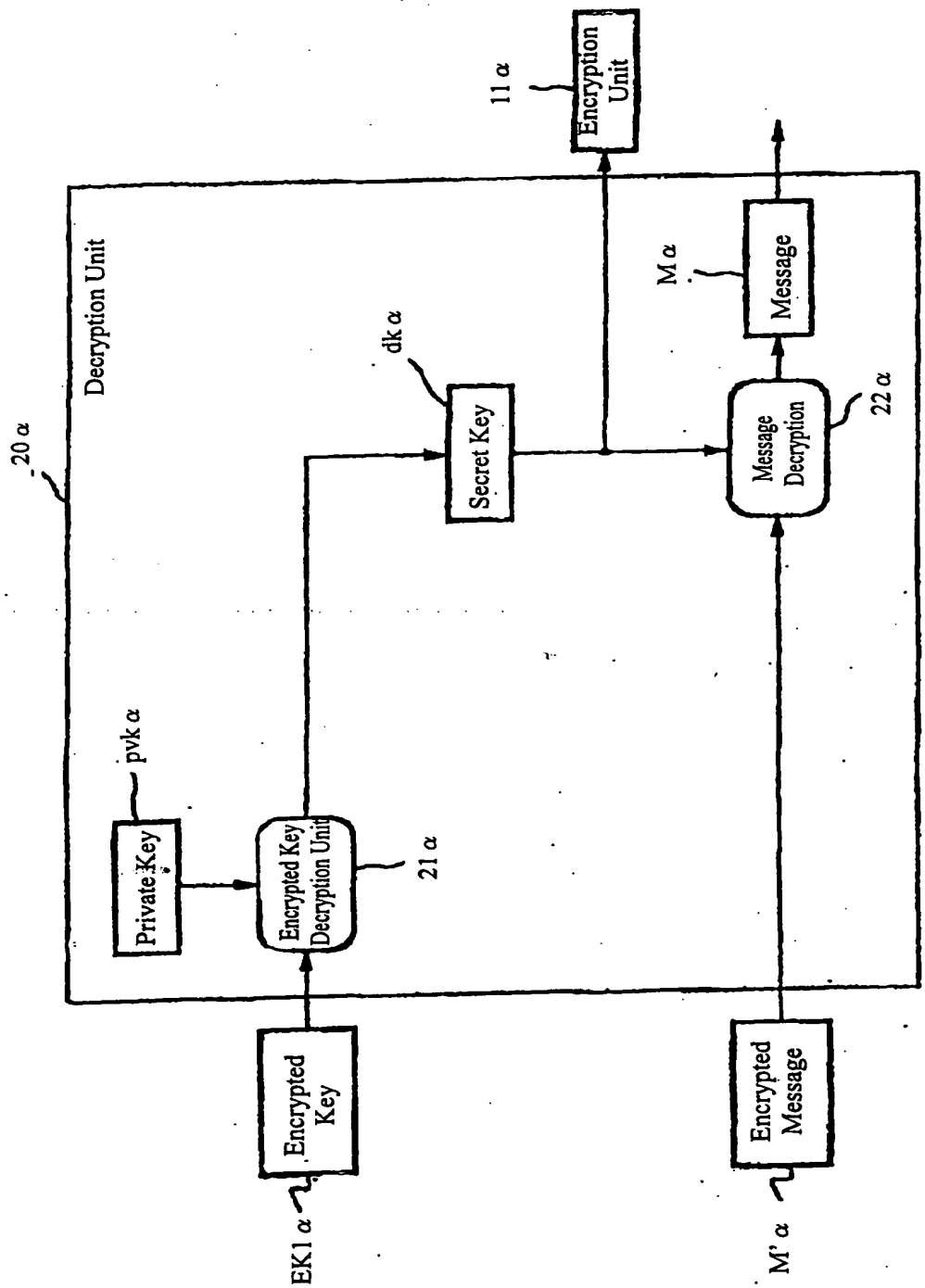
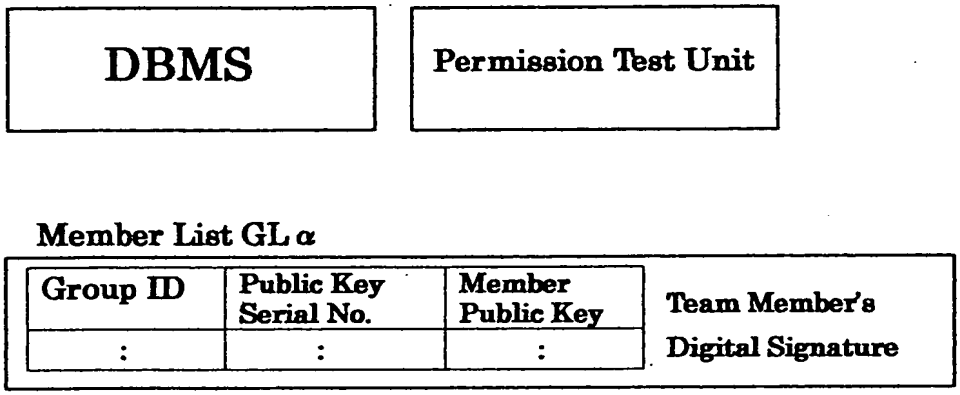

Data
Decryption Unit
20 α
Digital Signature Verification Unit
17 α
Digital Signature Affixing Unit
19 α
Public Key Administration Unit
18 α
Encrypted Key
Encrypted Key
Encrypted Key
Affixed Information
Encrypted Message
EK1 α
EK2 α
EKn α
aif α
16 α
13 α
Public Key
Public Key
Public Key
PK1 α
PK2 α
PKn α
Encripted Key Generation Unit
14 α
Affixed Information Generation Unit
15 α
12 α
Secret Key Generation Unit
Secret Key
11 α
Encryption Unit
M' α
10 α
M α
Message

FIG.3


Encryption Unit
11 α
Decryption Unit
20 α
Message
M α
dk α
Secret Key
Message Decryption
22 α
pvk α
Private Key
Encrypted Key Decryption Unit
21 α
Encrypted Key
EK1 α
Encrypted Message
M' α

09/700390

FIG.4



Member List GL α

Group ID	Public Key Serial No.	Member Public Key	Team Member's Digital Signature
:	:	:	

Secret Key List CKL α

Secret Key No.	Public Key Serial No.	Encrypted Key
122	11 : AA	qwer
122	1C : FF	zxcv
122	E5 : 4B	wurt

Group Secret Key List G CKL α

Group ID	Secret Key No.
B team	123

Encrypted Data List EDL α

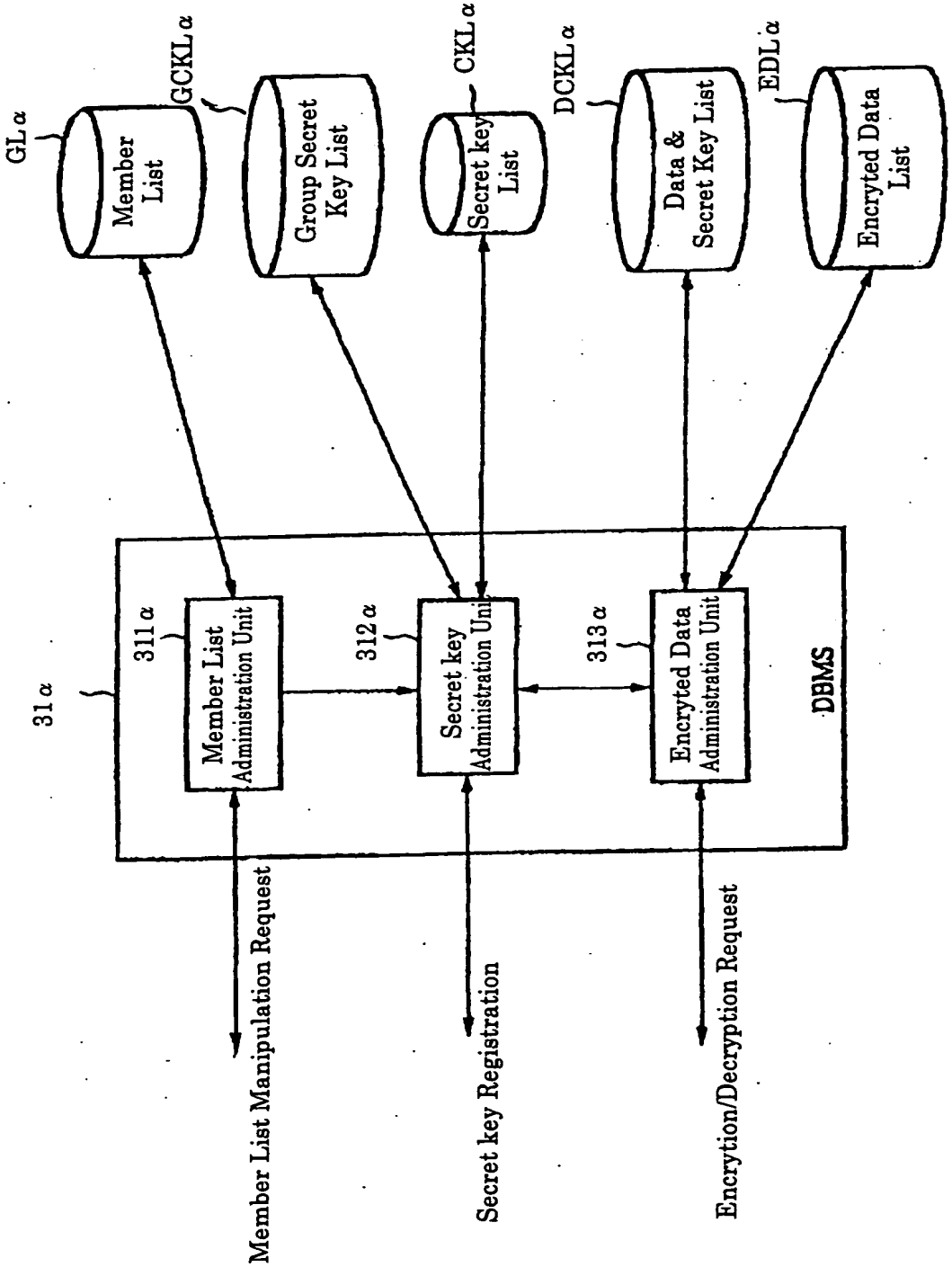
Data ID	Encrypted Data
4444	jjjjjjjjjjjjjjj

Data & Secret Key List DCKL α

Data ID	Secret Key No.
4444	123

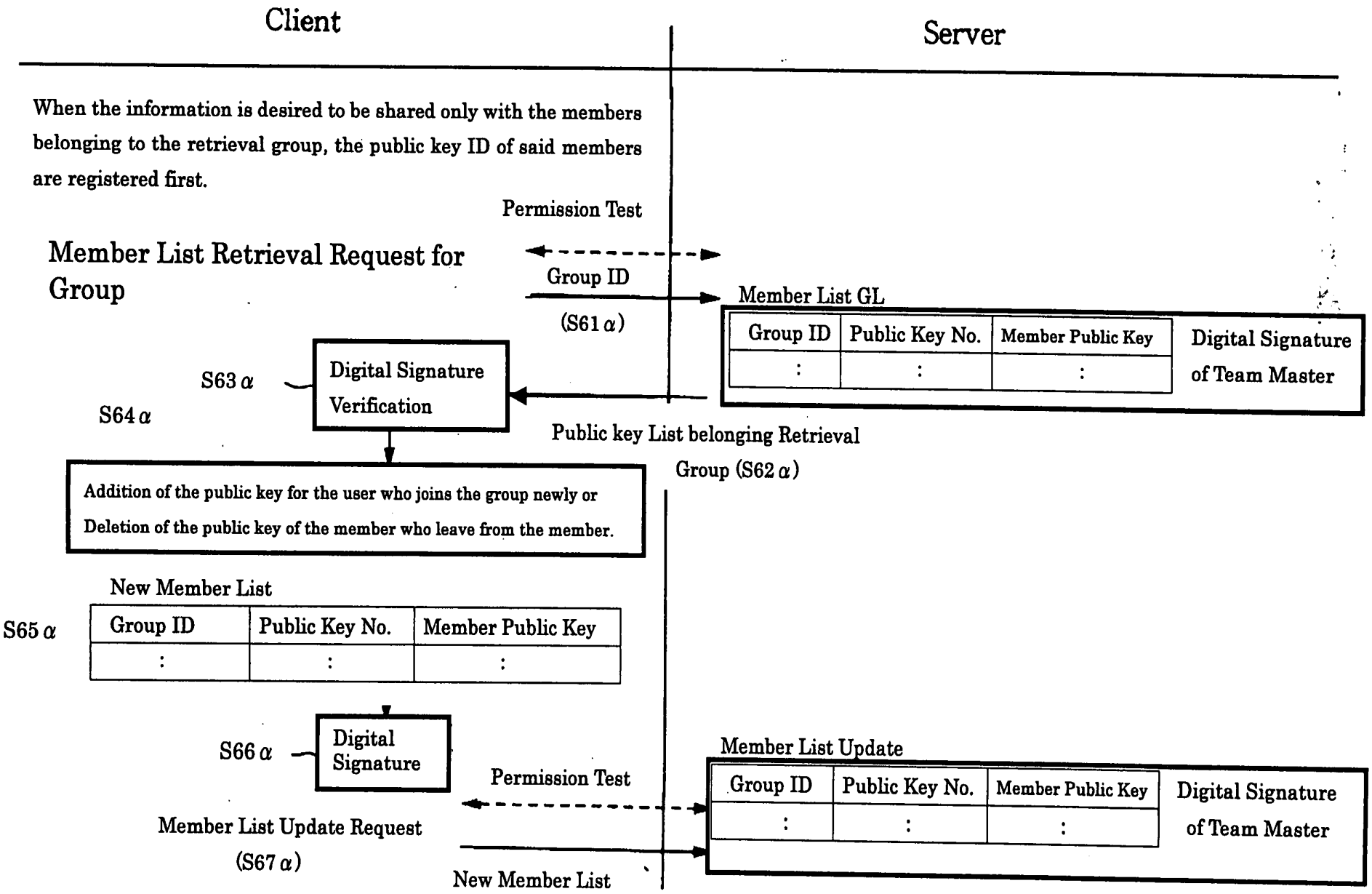
09/700390 09/700390 10/05/01

FIG.5


GL α
Member List
GCKL α
Group Secret Key List
CKL α
Secret key List
DCKL α
Data & Secret Key List
EDL α
Encryted Data List
31 α
311 α
Member List Administration Unit
312 α
Secret key Administration Unit
313 α
Encryted Data Administration Unit
DBMS
Member List Manipulation Request
Secret key Registration
Encrytion/Decryption Request

T09020*06E00260

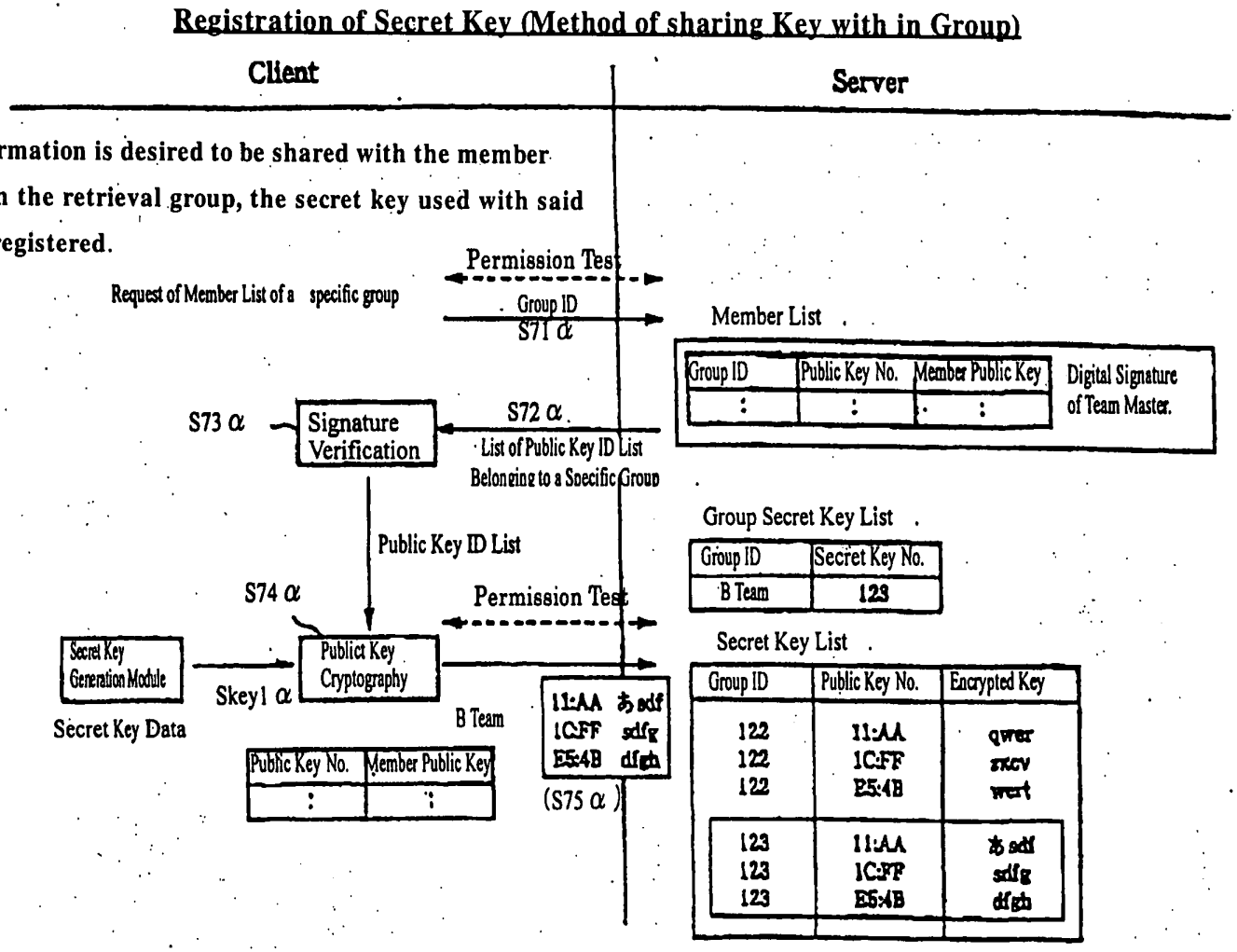
FIG.6 Example : Registration of Public key ID for Group (Method of sharing secret key within the group)



OBLON ET AL (703) 413-3000
DOCKET # 1984-1158 SHEET 6 OF 8
09/700390

T090Z0 "06E00Z60

FIG.7

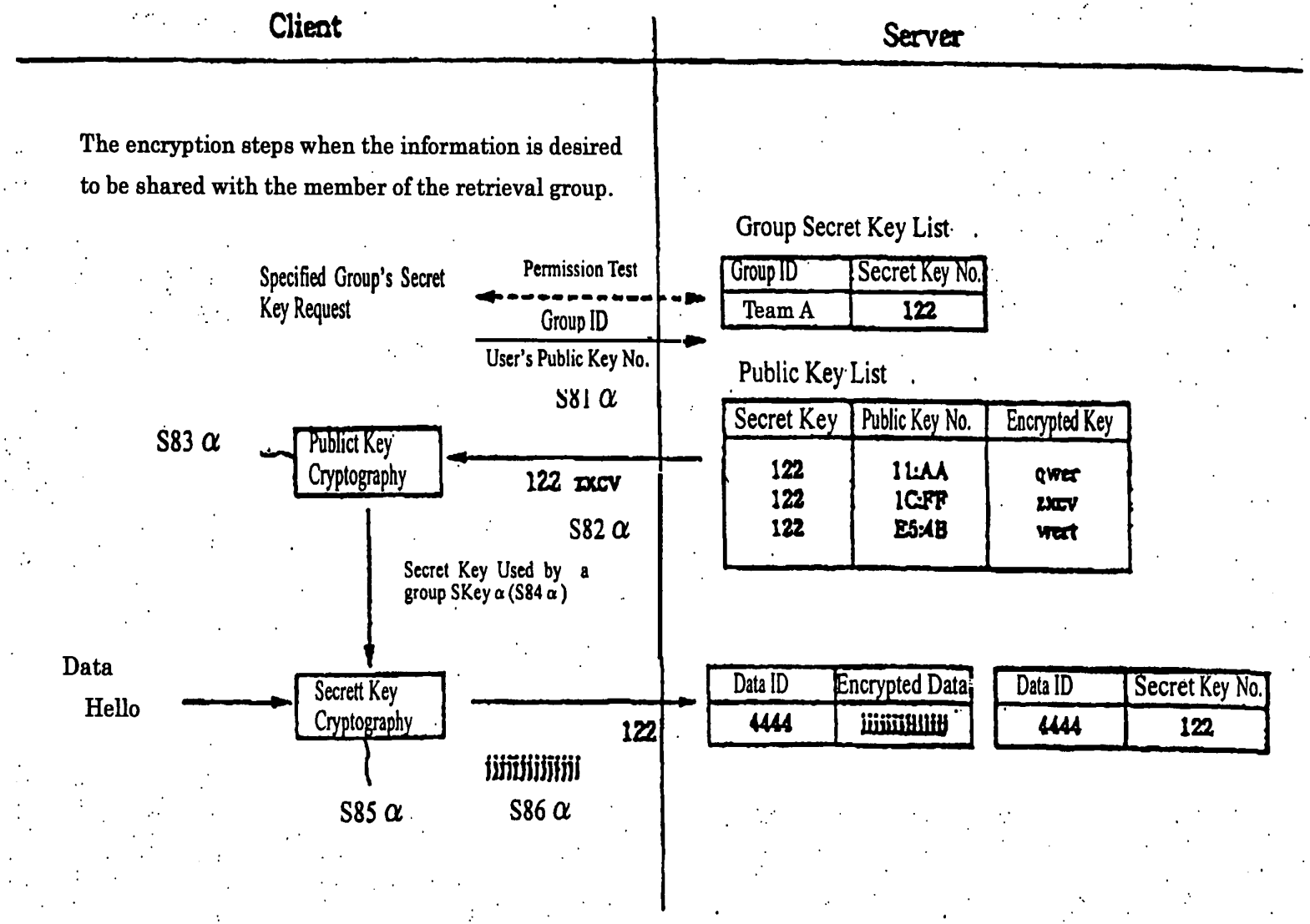


OBLON ET AL (703) 413-3000
DOCKET # 1614-0115US1 SHEET 7 OF 13
09/700390

T09070 "06E00760

FIG.8

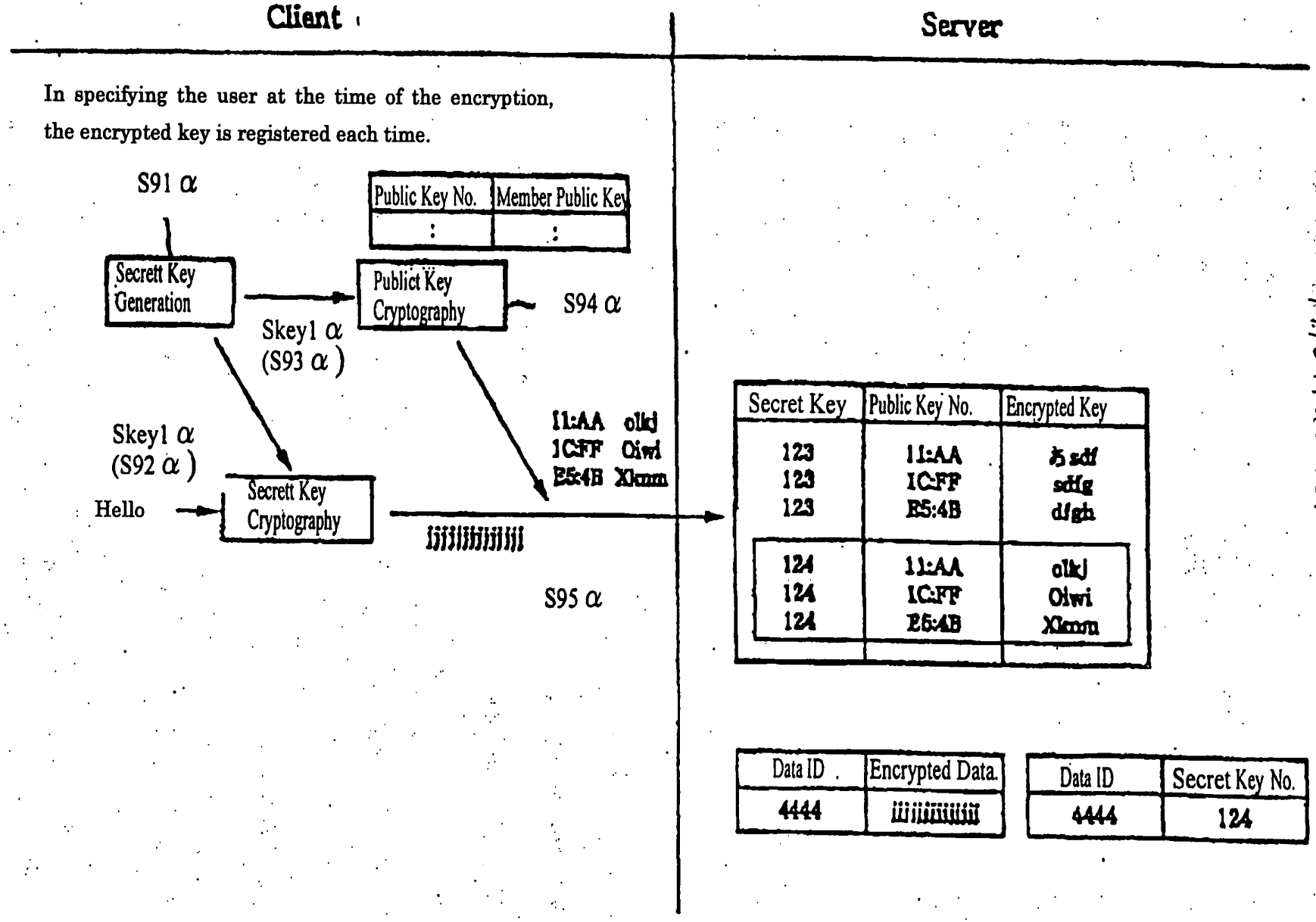
Example of Encryption (Method of Sharing Secret Key within Group)



OBLON ET AL (703) 413-3000
DOCKET # 199.1011US2PCT SHEET 8 OF 13
09/700390

T09070 06E00760

FIG. 9 Example of Encryption (Method of Sharing Secret Key with respectively selected user)

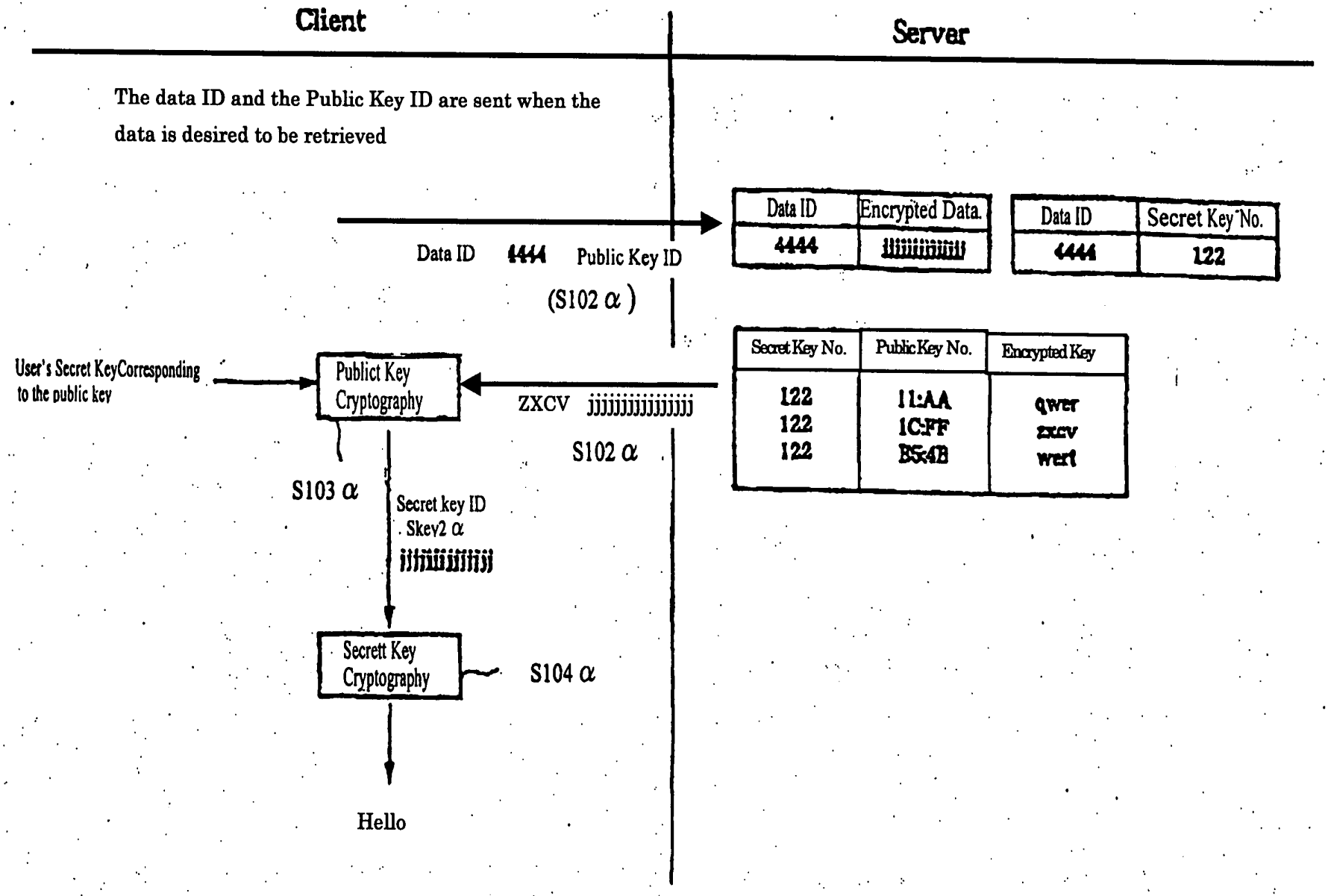


OBLON ET AL (703) 413-3000
DOCKET # 1946.1USAPT
SHEET 9 OF 10
09/700390

T09070 06E00760

FIG.10

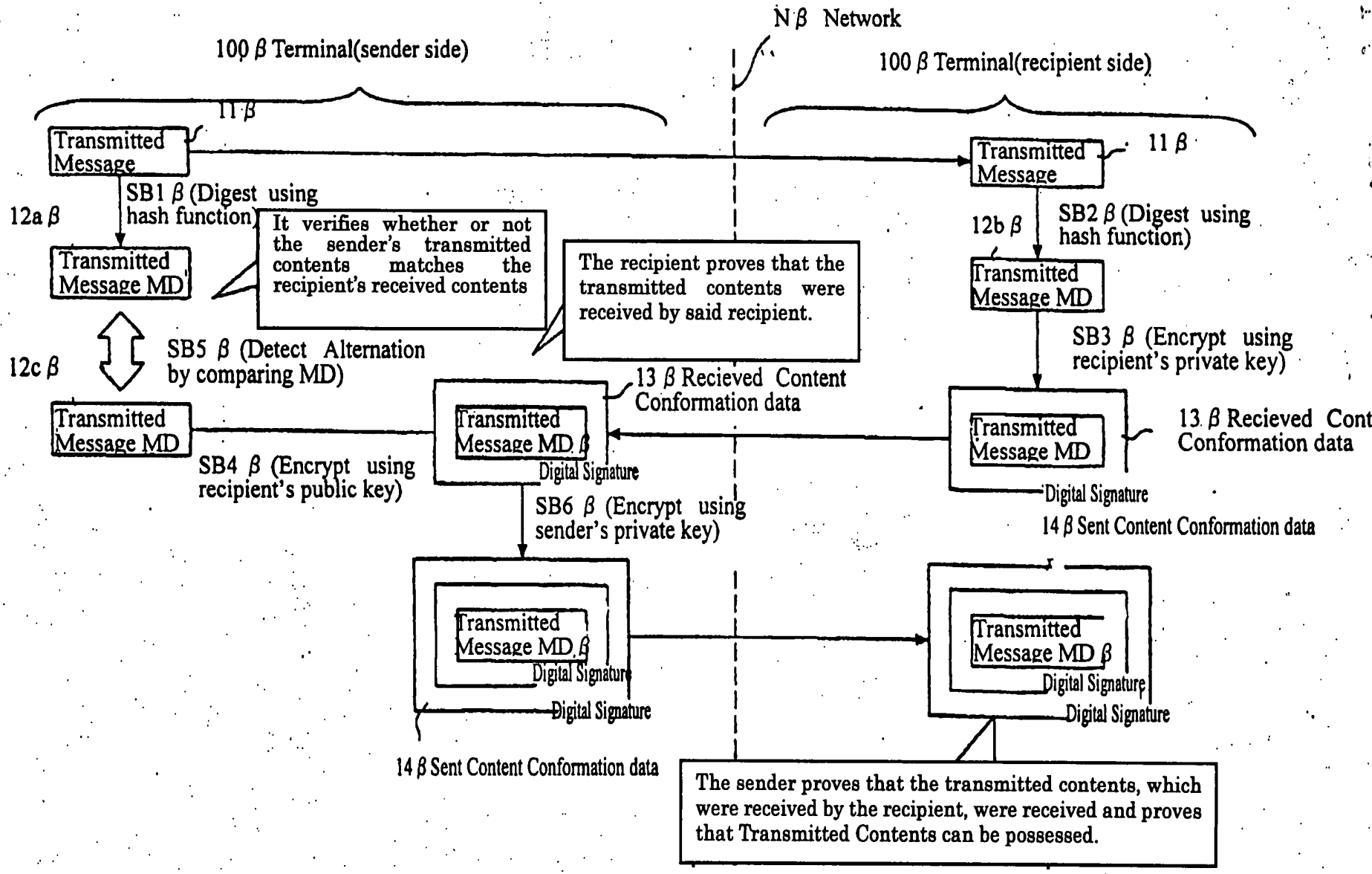
Example of Decryption (Both Case)



OBLON ET AL (703) 413-3000
DOCKET # 1998 US PCT
SHEET 10 OF 13
09/700390

T09020"06E00260

FIG11



OBLON ET AL (703) 413-3000
DOCKET # 19041/0028
SHEET 11 OF 13
09/700390

FIG12

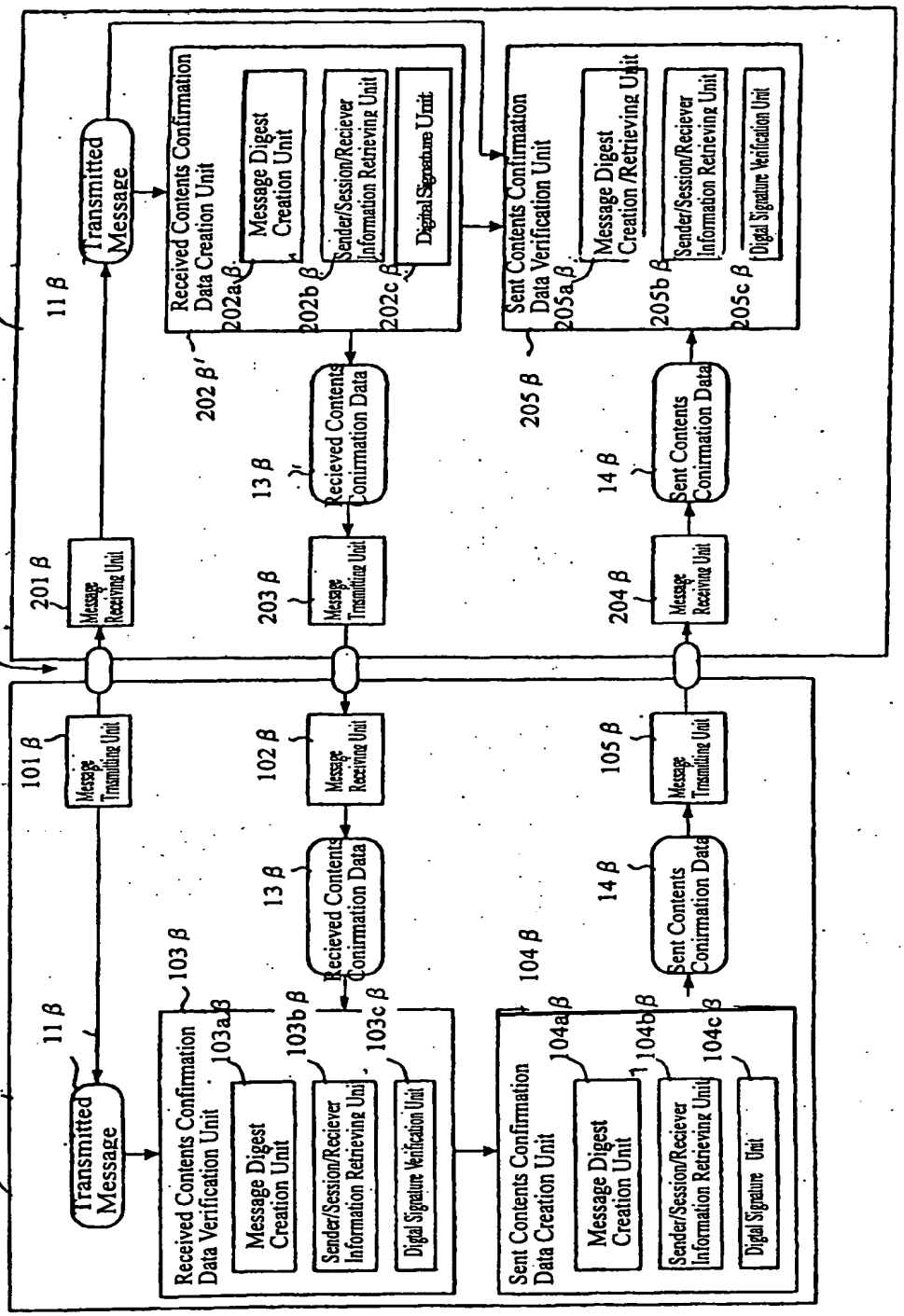
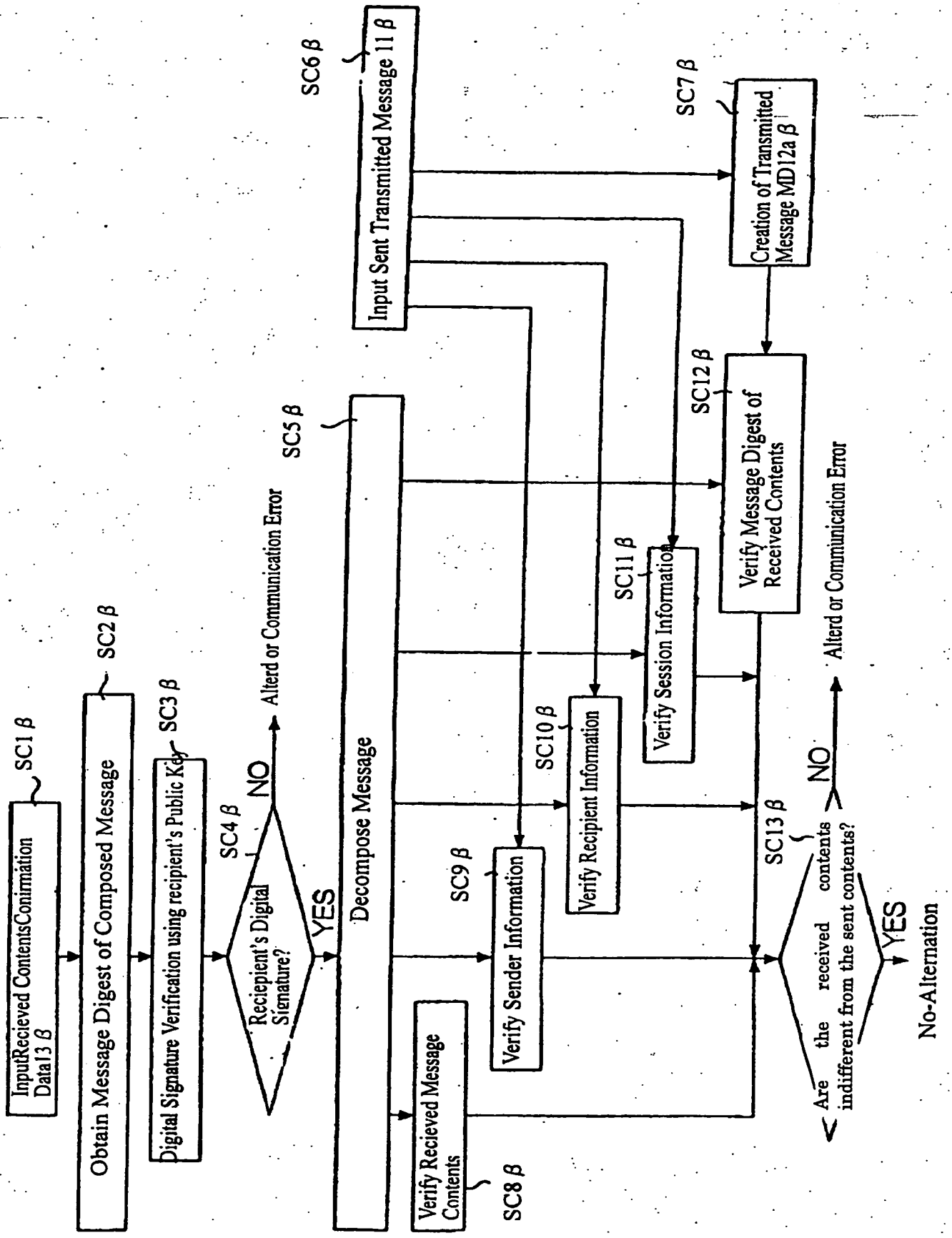
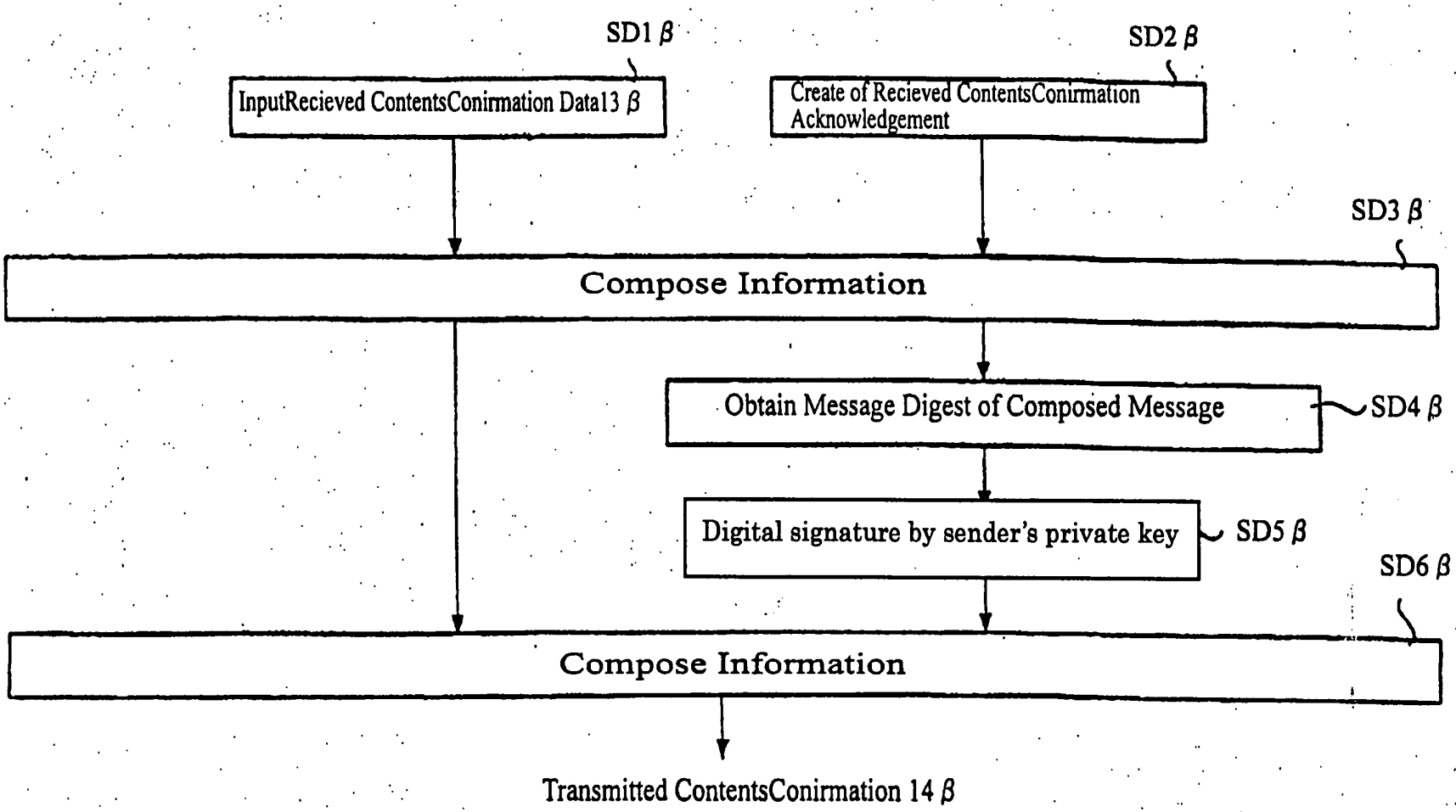

100 β Terminal(sender side)
200 β Terminal(recipient side)
N β Network
Transmitted Message
11 β
Message Transmitting Unit
101 β
Message Receiving Unit
201 β
Received Contents Confirmation Data Verification Unit
103 β
Message Digest Creation Unit
103a β
Sender/Session/Reciever Information Retrieving Unit
103b β
Digital Signature Verification Unit
103c β
Recieved Contents Conirmation Data
13 β
Message Receiving Unit
102 β
Message Transmitting Unit
203 β
Received Contents Confirmation Data Creation Unit
202 β'
Message Digest Creation Unit
202a β
Sender/Session/Reciever Information Retrieving Unit
202b β
Digital Signature Unit
202c β
Transmitted Message
11 β
Sent Contents Confirmation Data Creation Unit
104 β
Message Digest Creation Unit
104a β
Sender/Session/Reciever Information Retrieving Unit
104b β
Digital Signature Unit
104c β
Sent Contents Conirmation Data
14 β
Message Transmitting Unit
105 β
Message Receiving Unit
204 β
Sent Contents Confirmation Data Verification Unit
205 β
Message Digest Creation /Retrieving Unit
205a β
Sender/Session/Reciever Information Retrieving Unit
205b β
Digital Signature Verification Unit
205c β
Sent Contents Conirmation Data
14 β

FIG13


SC1 β
InputRecieved ContentsConimation Data13 β
SC2 β
Obtain Message Digest of Composed Message
SC3 β
Digital Signature Verification using recipient's Public Key
SC4 β
Reciepient's Digital Signature?
NO
Alterd or Communication Error
YES
SC5 β
Decompose Message
SC6 β
Input Sent Transmitted Message 11 β
SC7 β
Creation of Transmitted Message MD12a β
SC8 β
Verify Recieved Message Contents
SC9 β
Verify Sender Information
SC10 β
Verify Recipient Information
SC11 β
Verify Session Information
SC12 β
Verify Message Digest of Received Contents
SC13 β
Are the received contents indifferent from the sent contents?
NO
Alterd or Communication Error
YES
No-Alternation

09700390 "06E00760

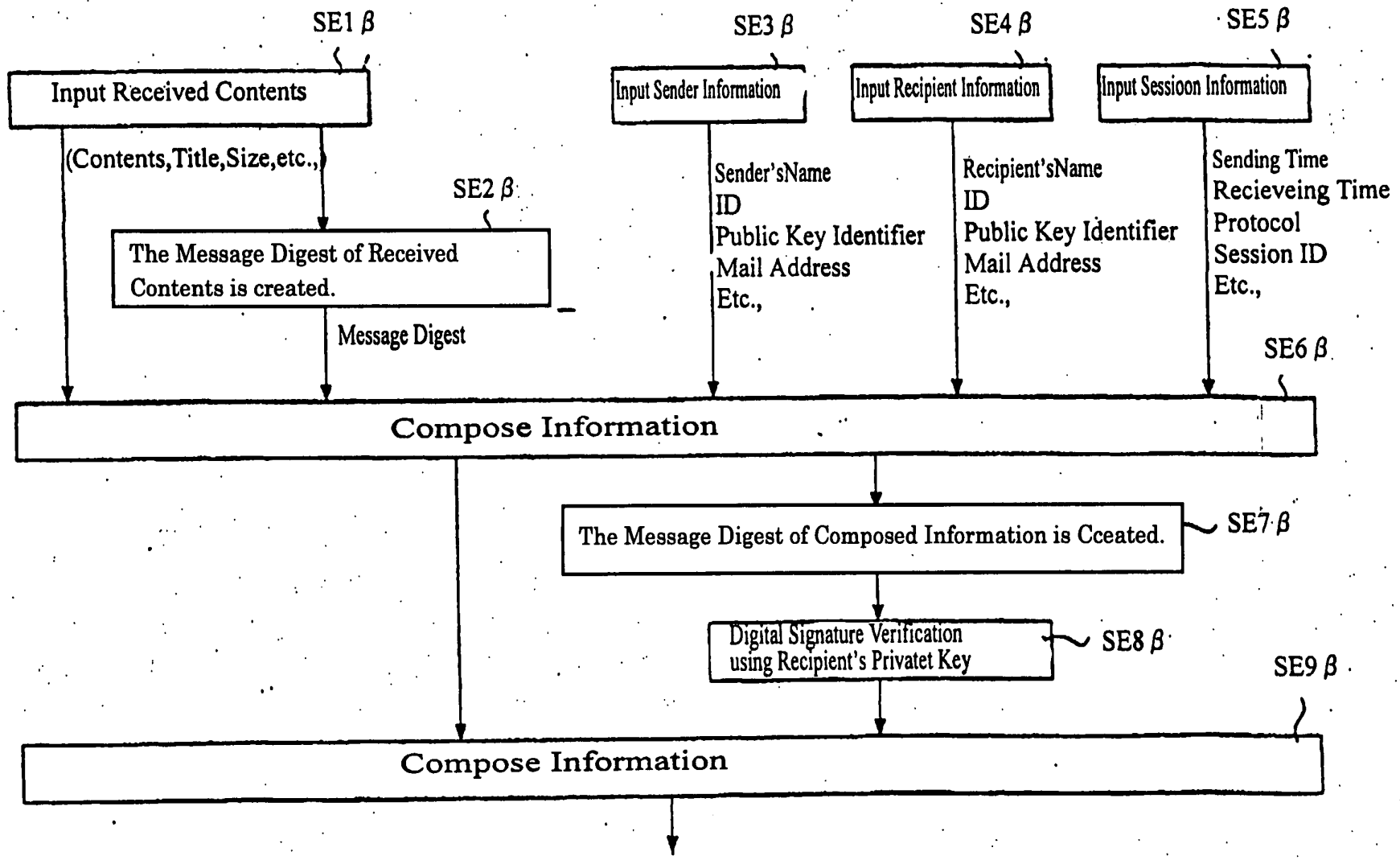
FIG14



OBLON ET AL (703) 413-3000
DOCKET # 1990 AUS RG
SHEET 14 OF 23
09/700390

T09070 06E00760

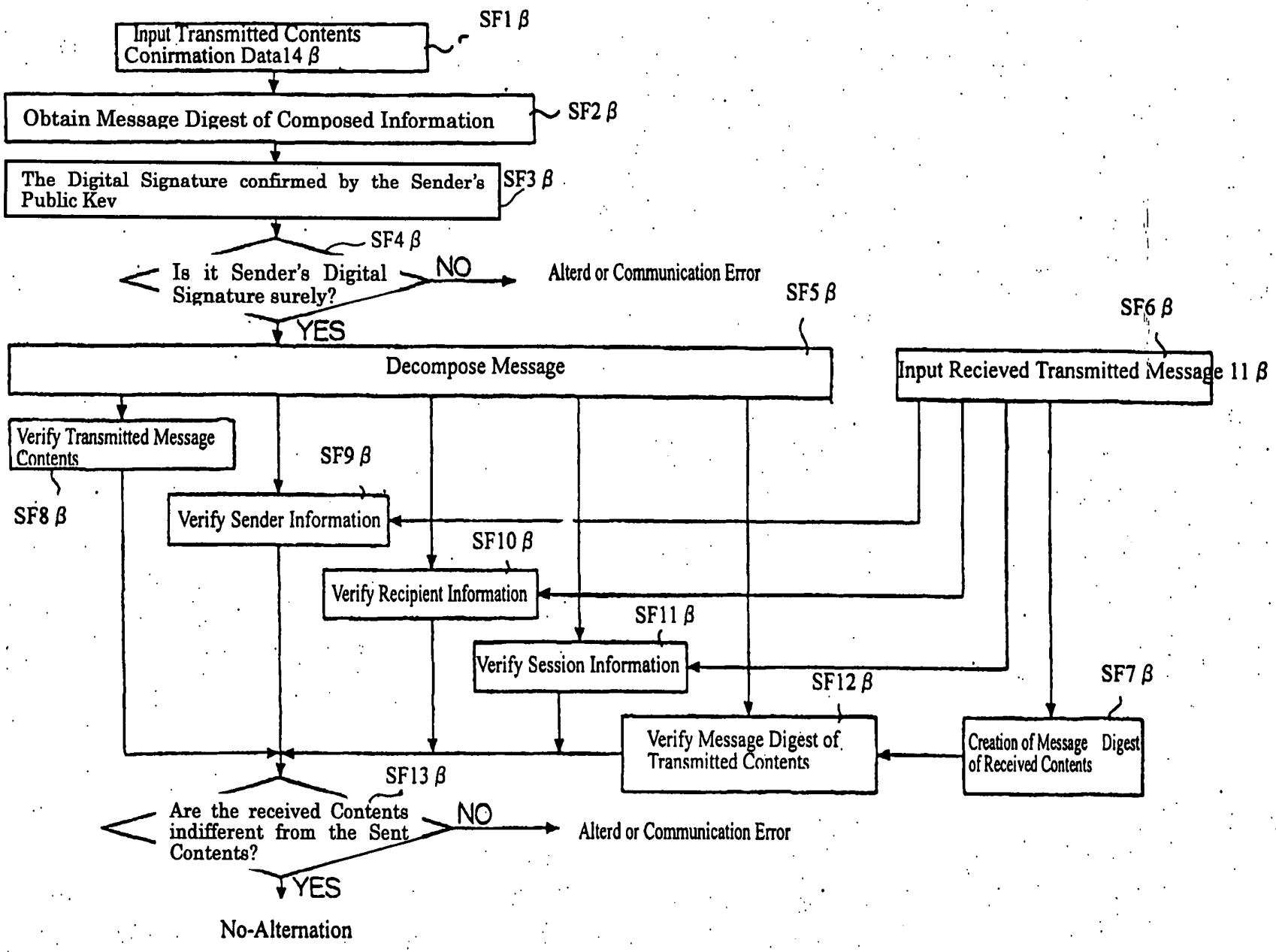
FIG15



OBLON ET AL (703) 413-3000
DOCKET # 1990.1.US.01
SHEET 15 OF 23
09/700390

T09070 06E0076D

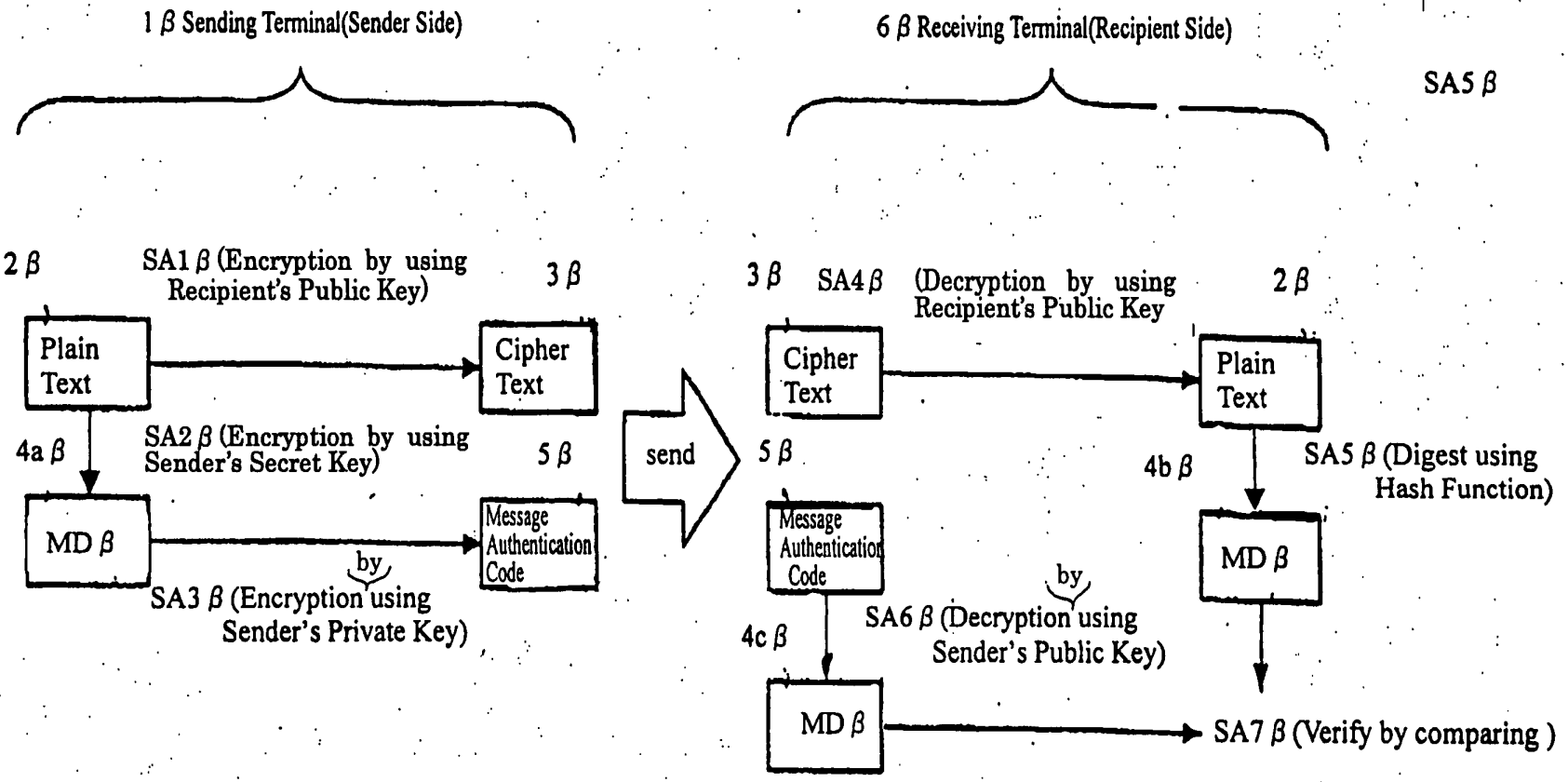
FIG16



OBLON ET AL (703) 413-3000
DOCKET # 09/700390
SHEET 16 OF 17
09/700390

09700390 "060007"

FIG17



OBLON ET AL (703) 413-3000
DOCKET # 199681US2PCT
SHEET 17 OF 73
09/700390

FIG18

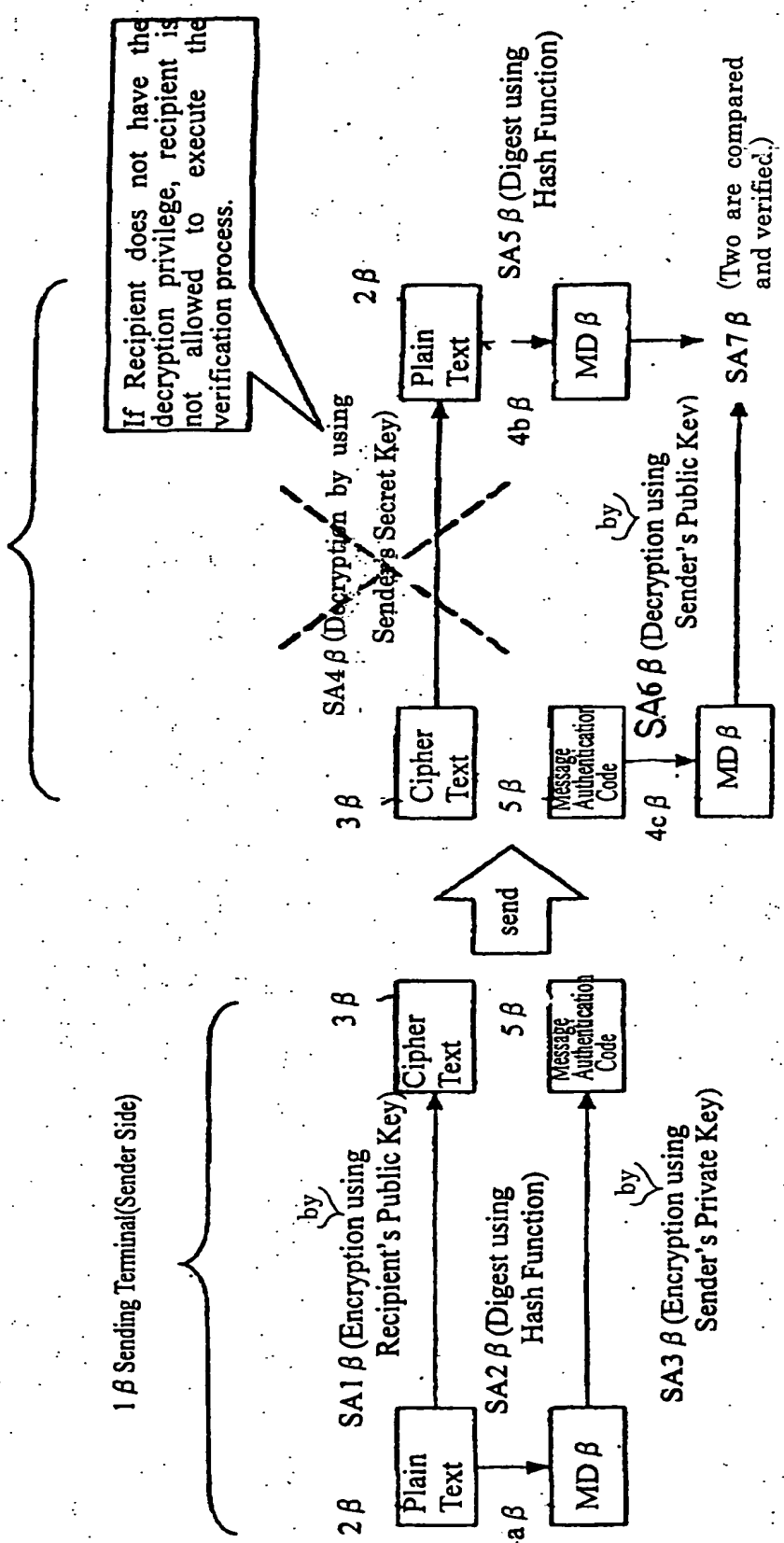
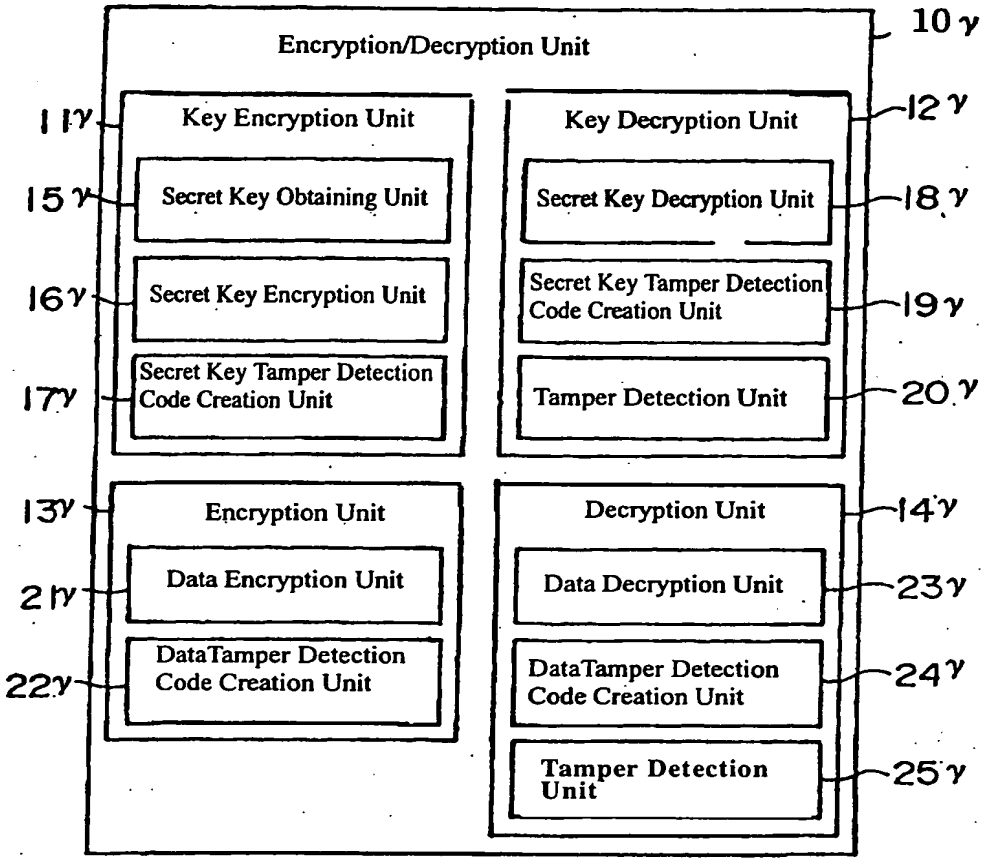

1 β Sending Terminal(Sender Side)
2 β
Plain Text
4a β
MD β
SA1 β (Encryption using Recipient's Public Key)
by
SA2 β (Digest using Hash Function)
SA3 β (Encryption using Sender's Private Key)
by
3 β
Cipher Text
5 β
Message Authentication Code
send
6 β Receiving Terminal(Recipient Side)
If Recipient does not have the decryption privilege, recipient is not allowed to execute the verification process.
SA4 β (Decryption by using Sender's Secret Key)
2 β
Plain Text
SA5 β (Digest using Hash Function)
4b β
MD β
by
SA6 β (Decryption using Sender's Public Key)
4c β
MD β
SA7 β (Two are compared and verified.)

FIG.19



P09700390

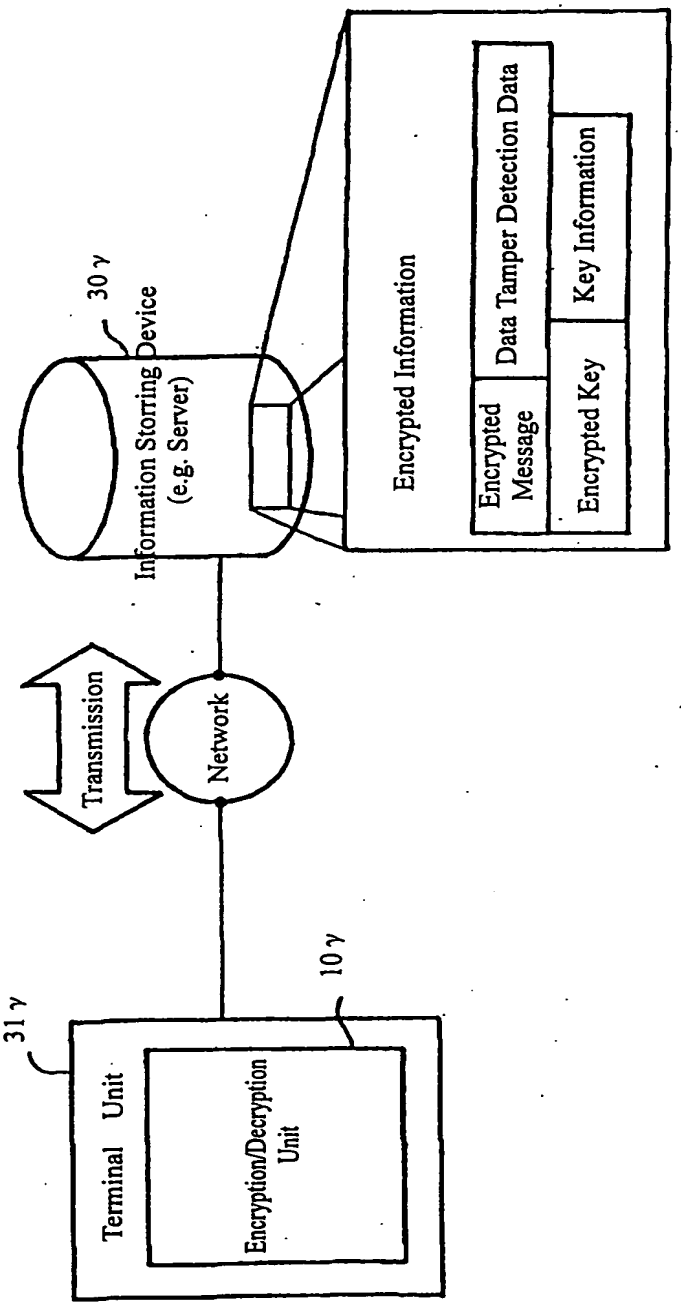
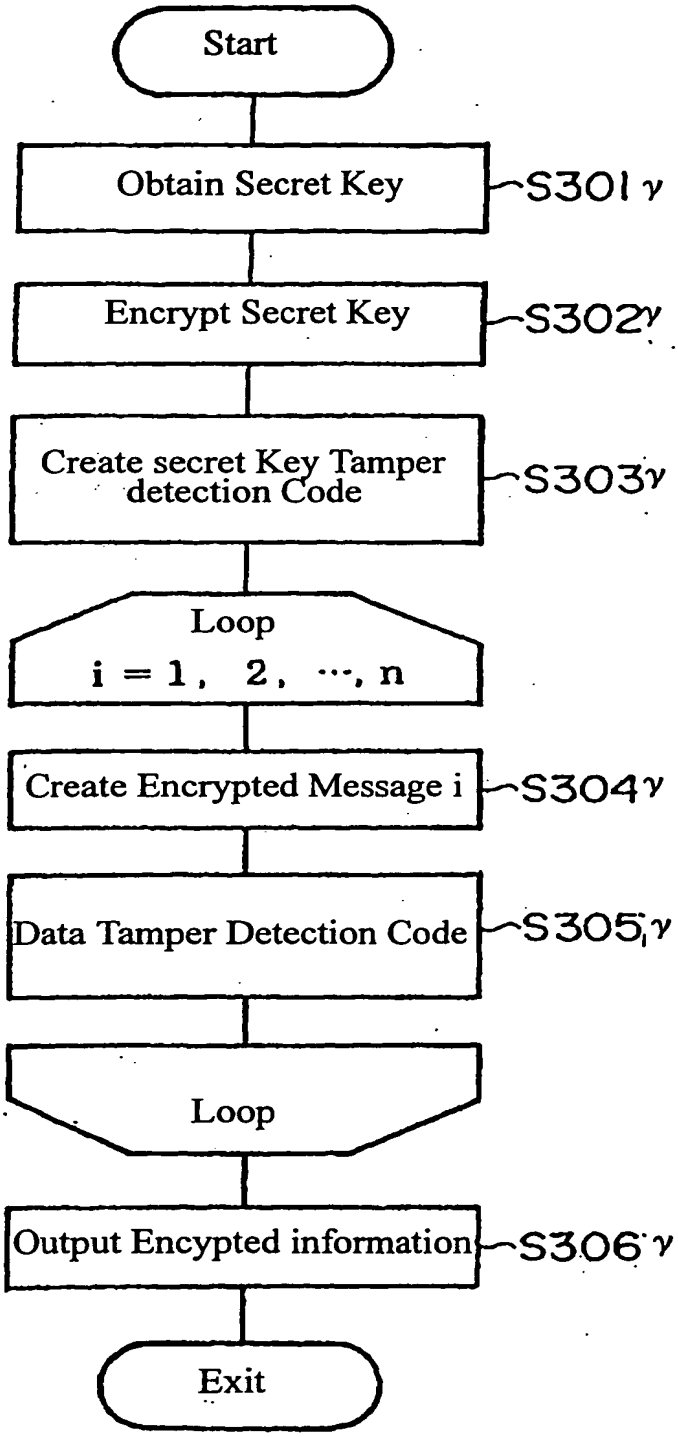


FIG20

T09040 "05E0450

FIG.21


Start
Obtain Secret Key
S301
Encrypt Secret Key
S302
Create secret Key Tamper detection Code
S303
Loop
i = 1, 2, ···, n
Create Encrypted Message i
S304
Data Tamper Detection Code
S305
Loop
Output Encypted information
S306
Exit

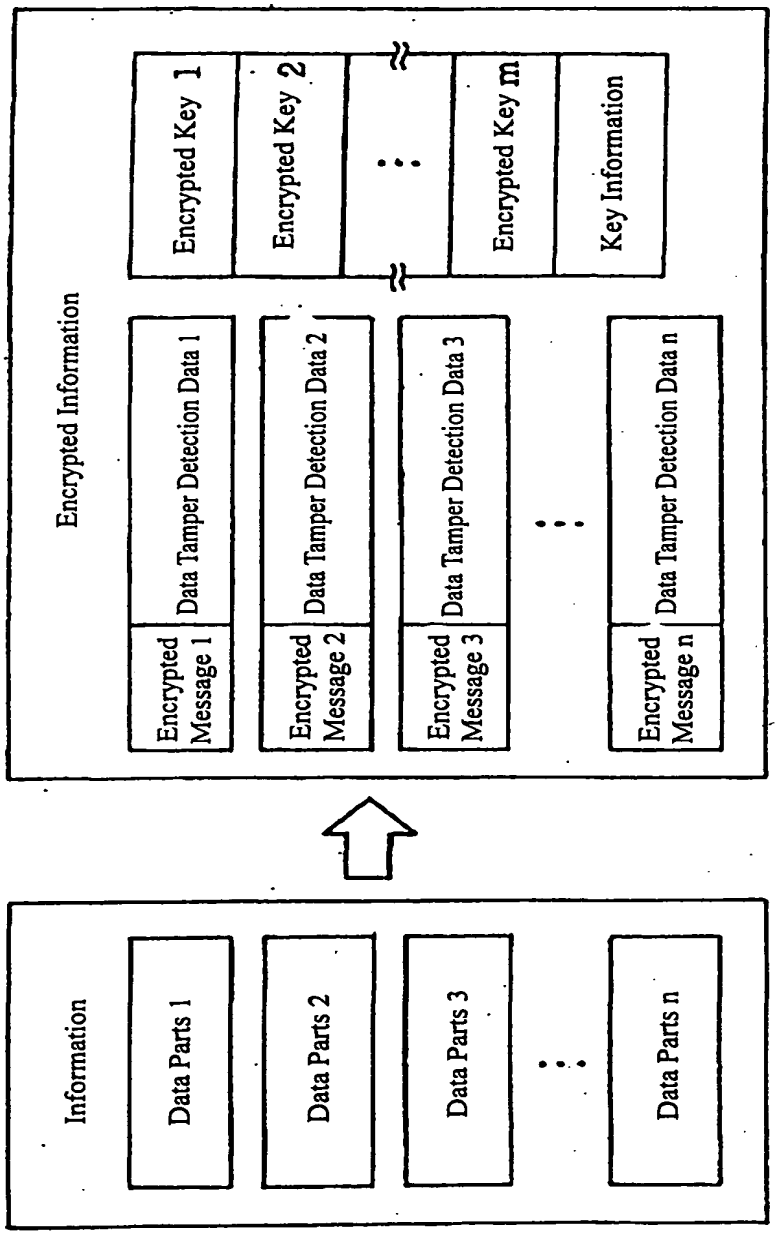


FIG22

T0940 "05C0060

FIG.23

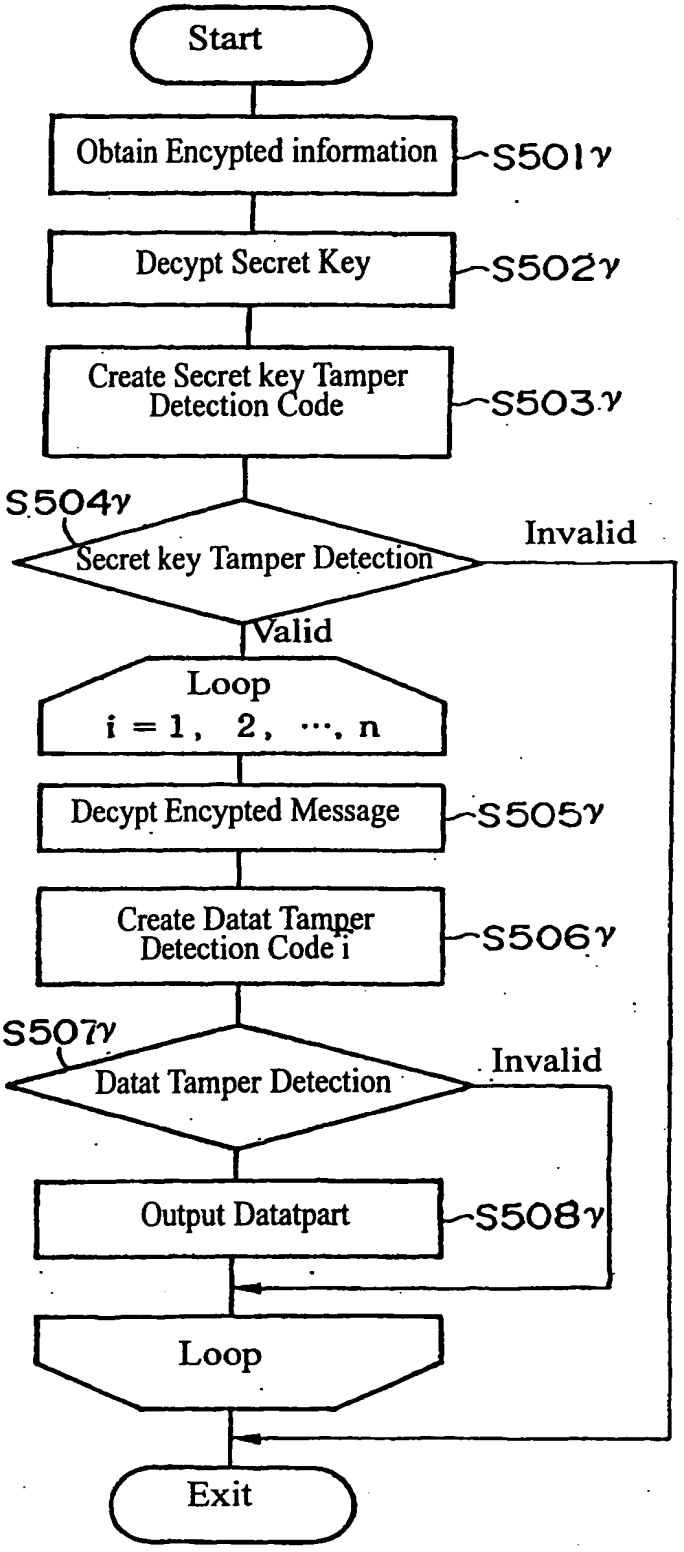
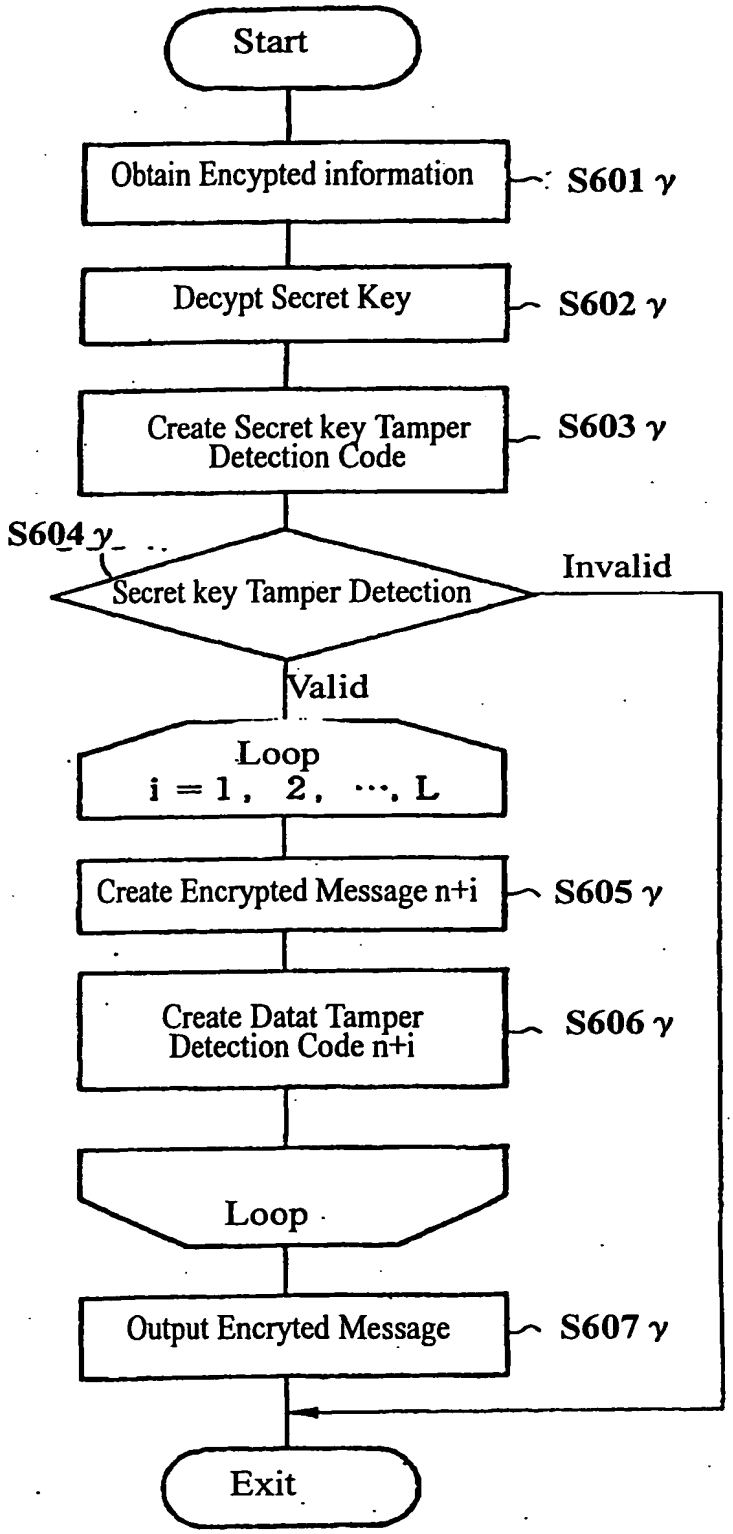
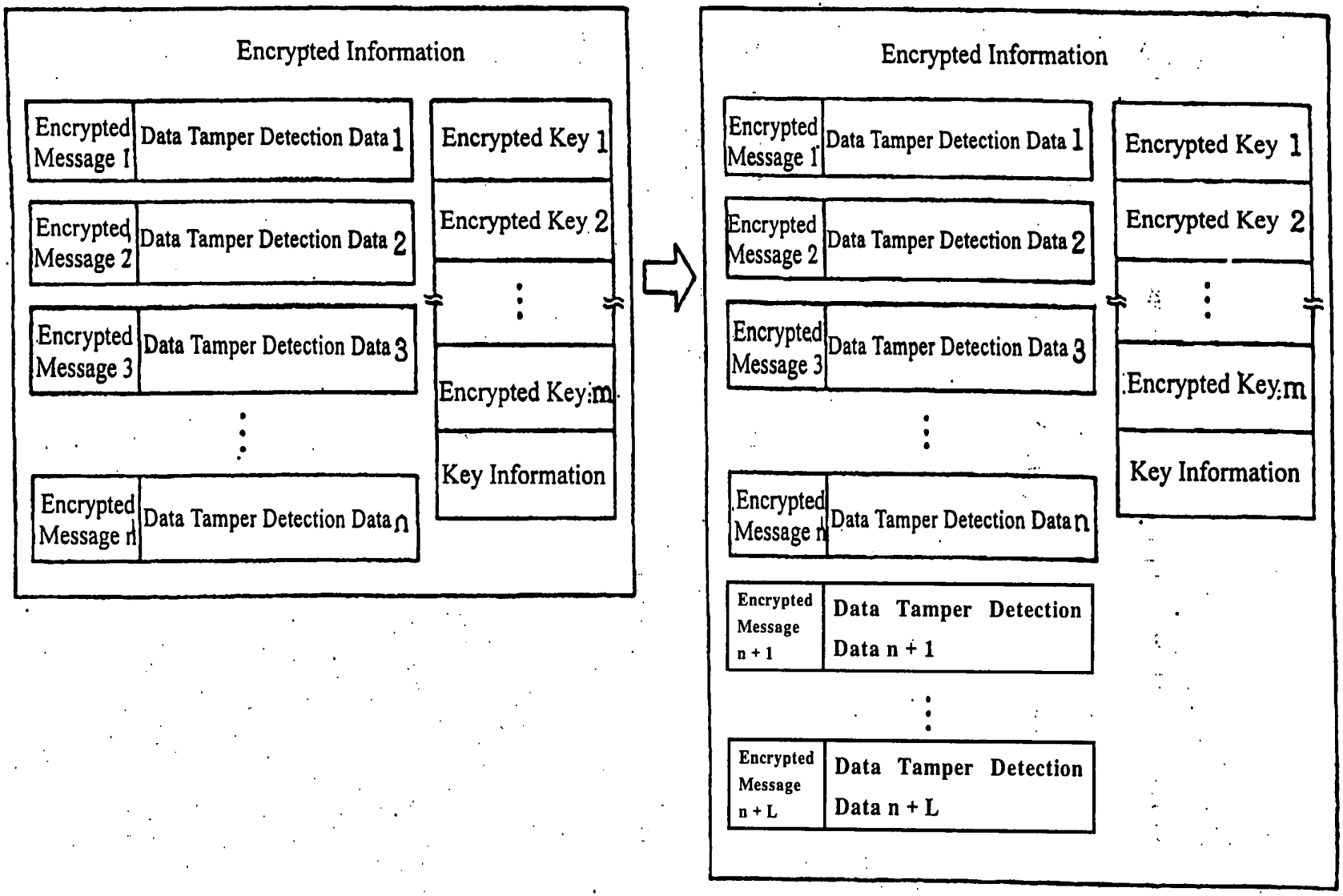

Start
Obtain Encypted information
S501γ
Decypt Secret Key
S502γ
Create Secret key Tamper Detection Code
S503γ
S504γ
Secret key Tamper Detection
Invalid
Valid
Loop
i = 1, 2, ···, n
Decypt Encypted Message
S505γ
Create Datat Tamper Detection Code i
S506γ
S507γ
Datat Tamper Detection
Invalid
Output Datatpart
S508γ
Loop
Exit

FIG.24


Start
Obtain Encypted information
S601 γ
Decypt Secret Key
S602 γ
Create Secret key Tamper Detection Code
S603 γ
S604 γ
Secret key Tamper Detection
Invalid
Valid
Loop
i = 1, 2, ···, L
Create Encrypted Message n+i
S605 γ
Create Datat Tamper Detection Code n+i
S606 γ
Loop
Output Encryted Message
S607 γ
Exit

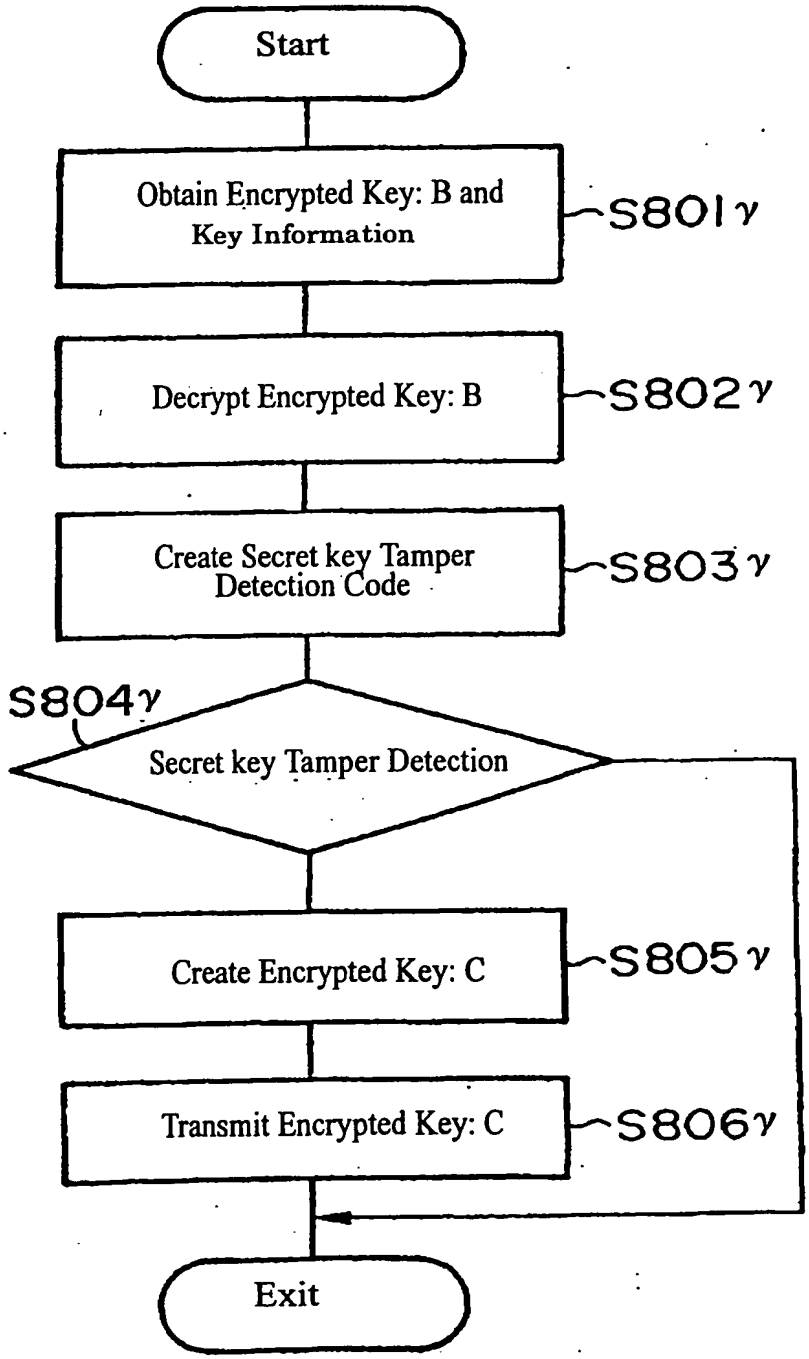
T090270 06E00760

FIG25



OBLON ET AL (703) 413-3000
DOCKET # [illegible]
SHEET 25 OF 73
09/700390

FIG.26


Start
Obtain Encrypted Key: B and Key Information
S801
Decrypt Encrypted Key: B
S802
Create Secret key Tamper Detection Code
S803
S804
Secret key Tamper Detection
Create Encrypted Key: C
S805
Transmit Encrypted Key: C
S806
Exit

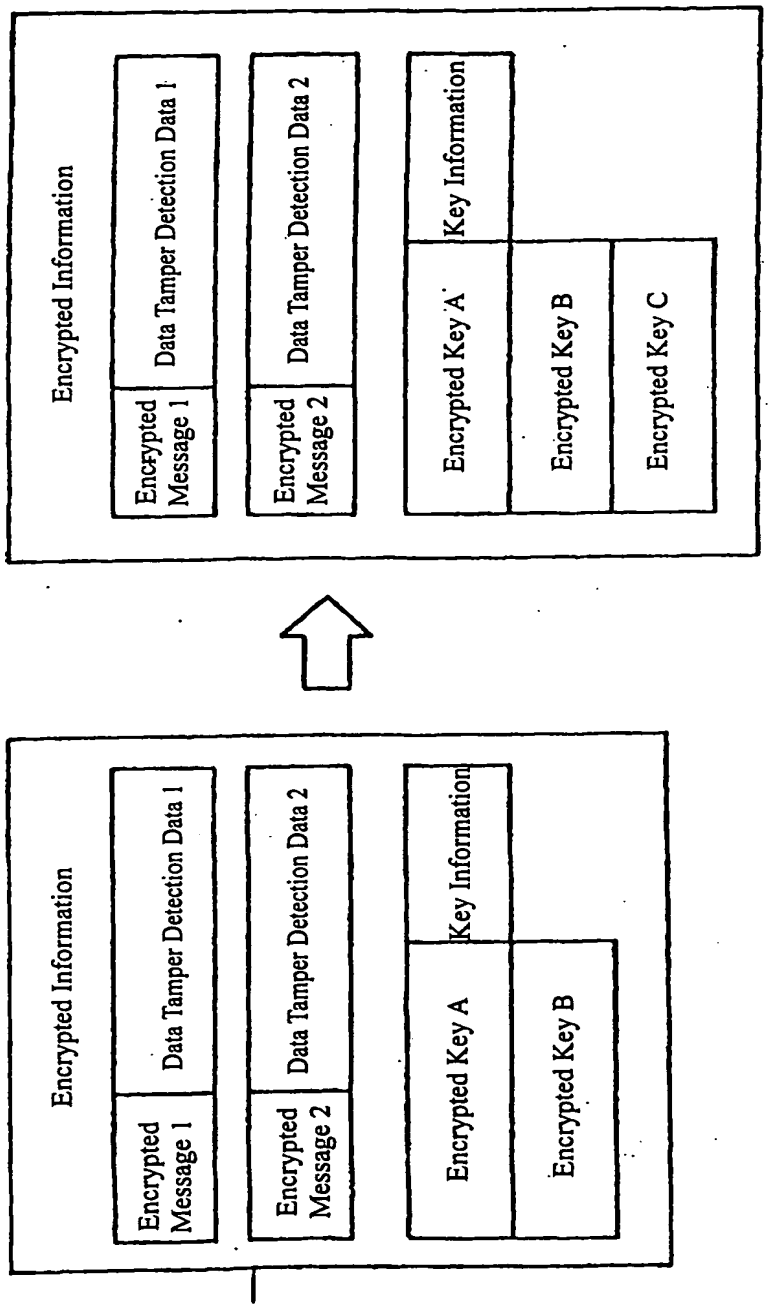
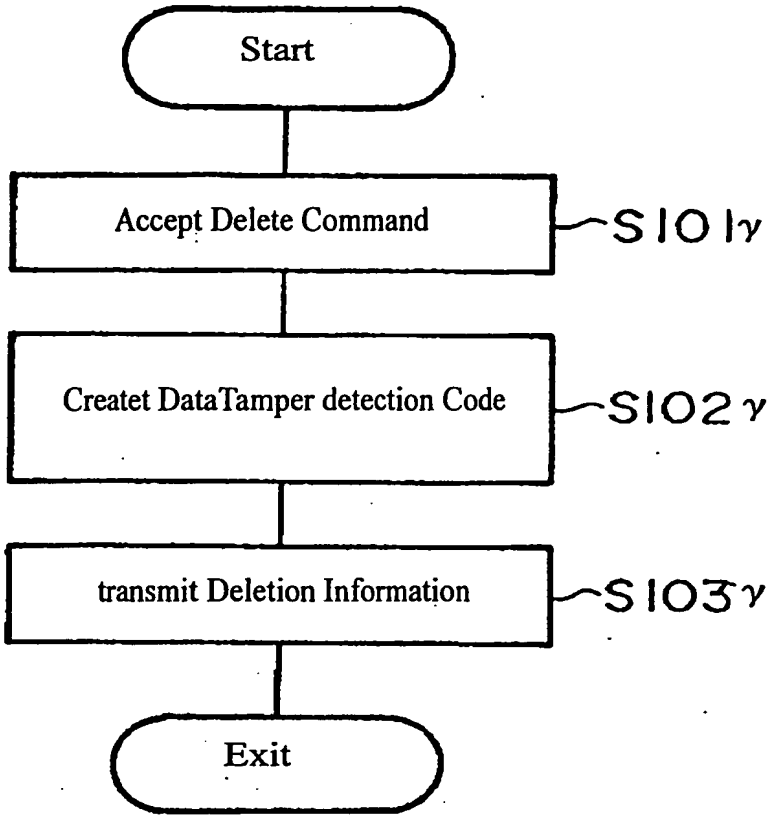


FIG27

T0901.0 "05.00.60

FIG.28



EP0907105A2 I

T0960 "05E0650

FIG29

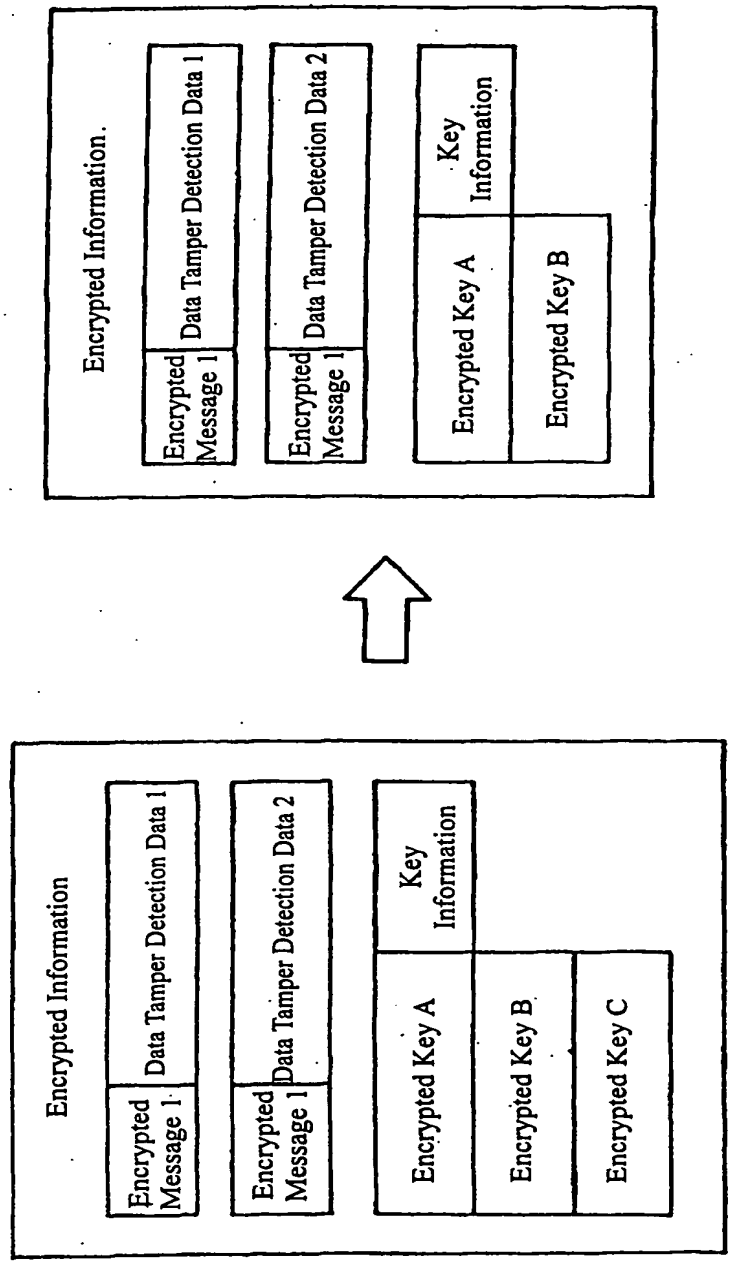


FIG.30

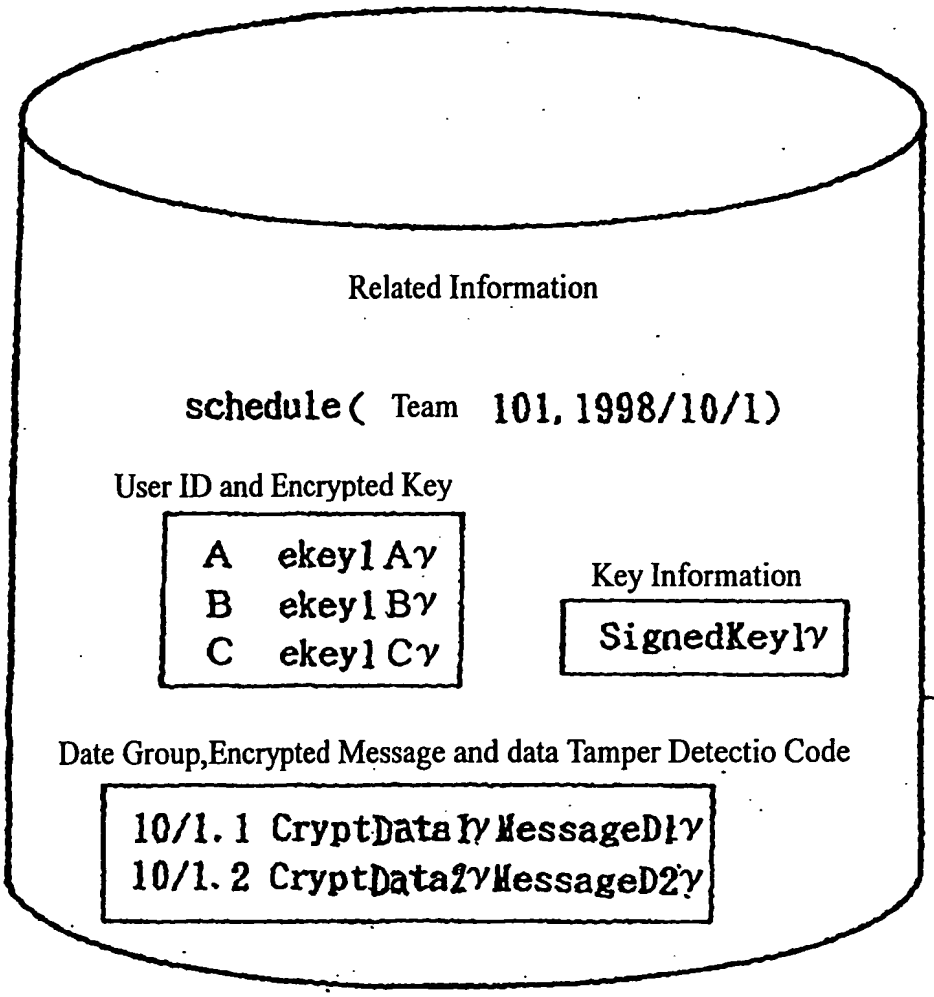
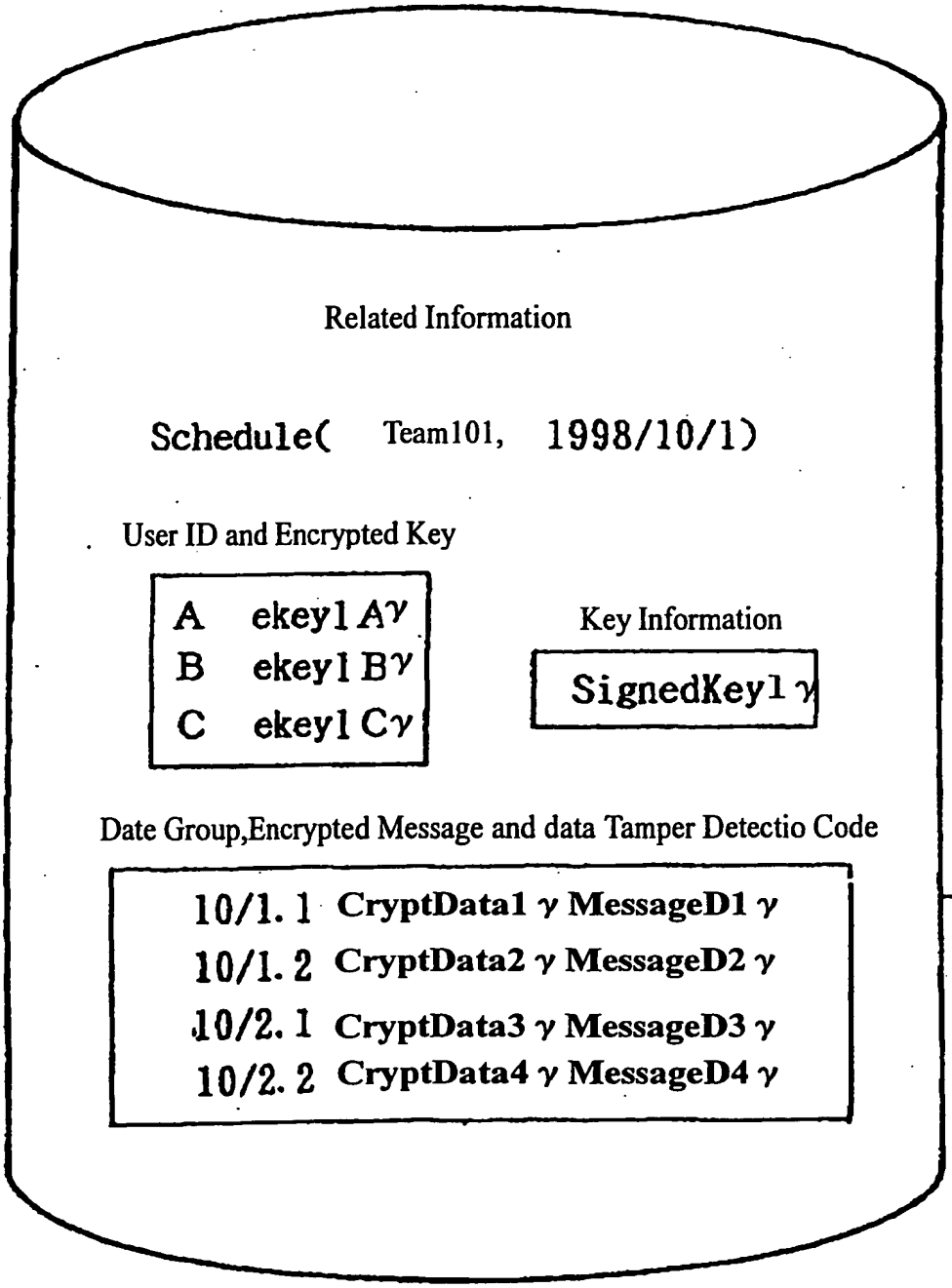

Related Information
schedule(Team 101, 1998/10/1)
User ID and Encrypted Key
A ekey1Aγ
B ekey1Bγ
C ekey1Cγ
Key Information
SignedKey1γ
Information Storing device
30γ
Date Group,Encrypted Message and data Tamper Detectio Code
10/1.1 CryptData1γMessageD1γ
10/1.2 CryptData2γMessageD2γ

FIG.31



T090720 "05300260

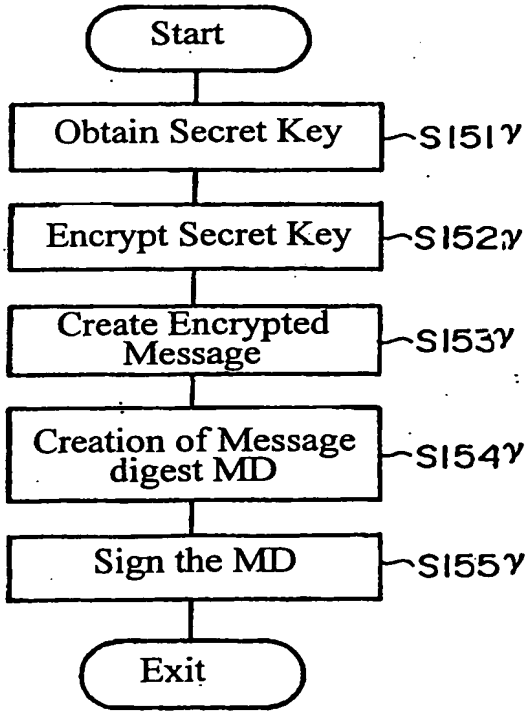
FIG.32

Team101 : Schedule

Oct.

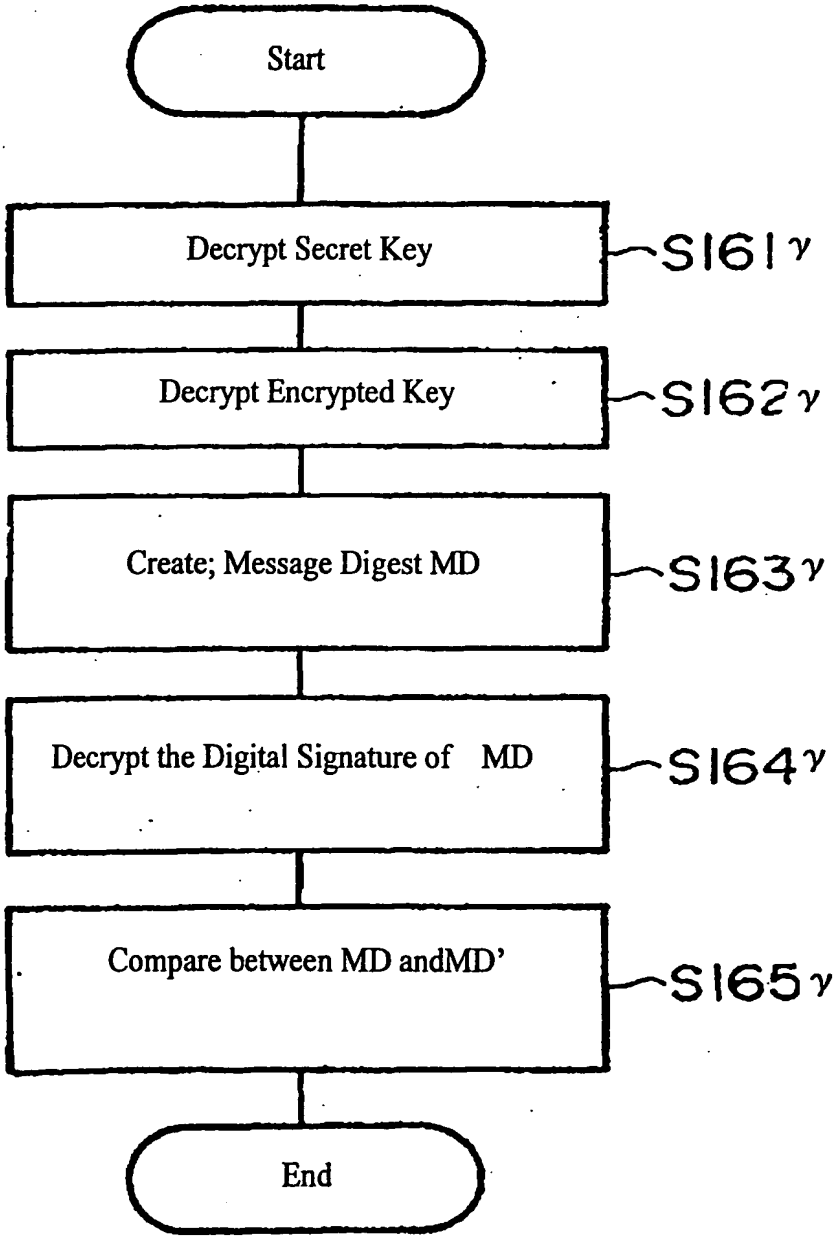
1 B : Go to Seminar 15:00~	2 A : Meeting 17:00~	

FIG.33



09/700390

FIG.34



09700390 "09/700390

FIG.35

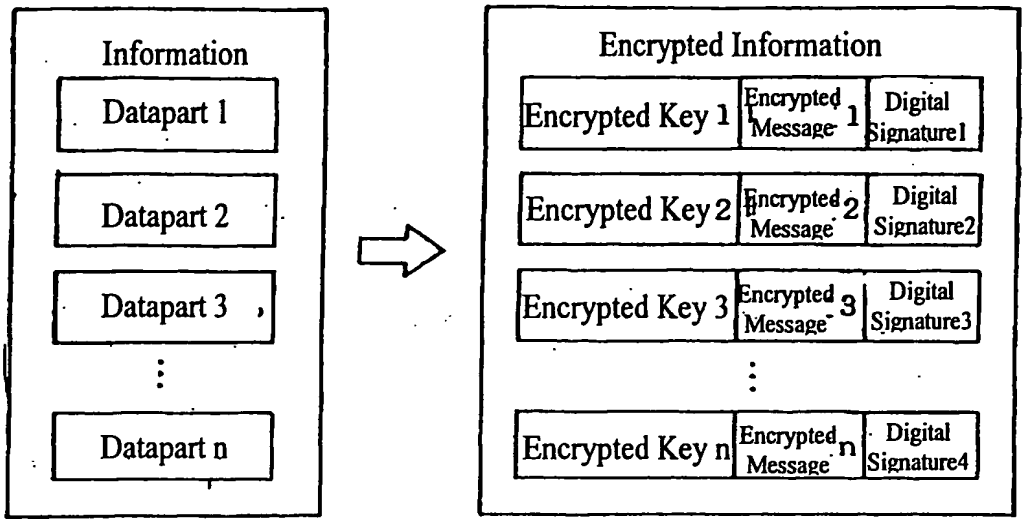

Information
Datapart 1
Datapart 2
Datapart 3
Datapart n
Encrypted Information
Encrypted Key 1
Encrypted Message 1
Digital Signature1
Encrypted Key 2
Encrypted Message 2
Digital Signature2
Encrypted Key 3
Encrypted Message 3
Digital Signature3
Encrypted Key n
Encrypted Message n
Digital Signature4

FIG.36

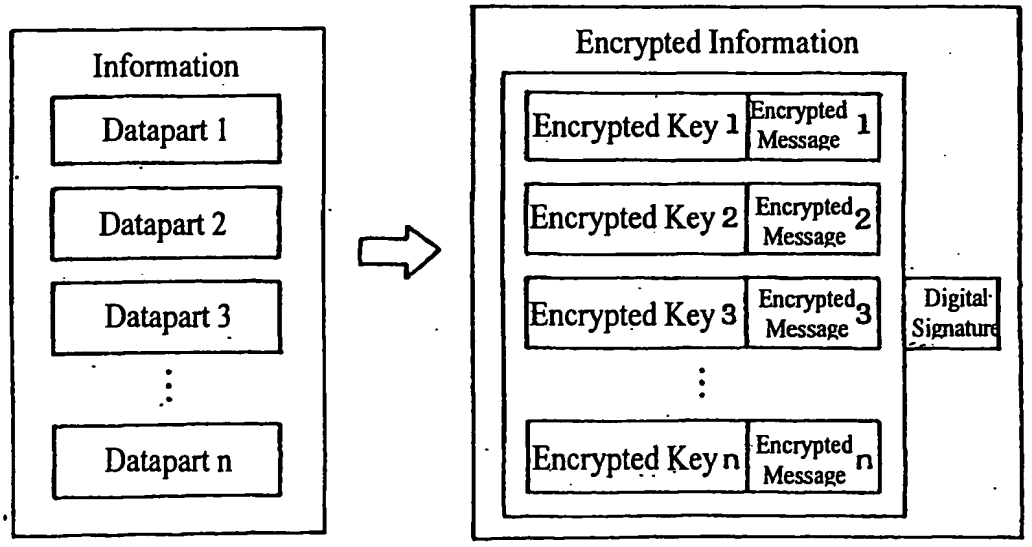
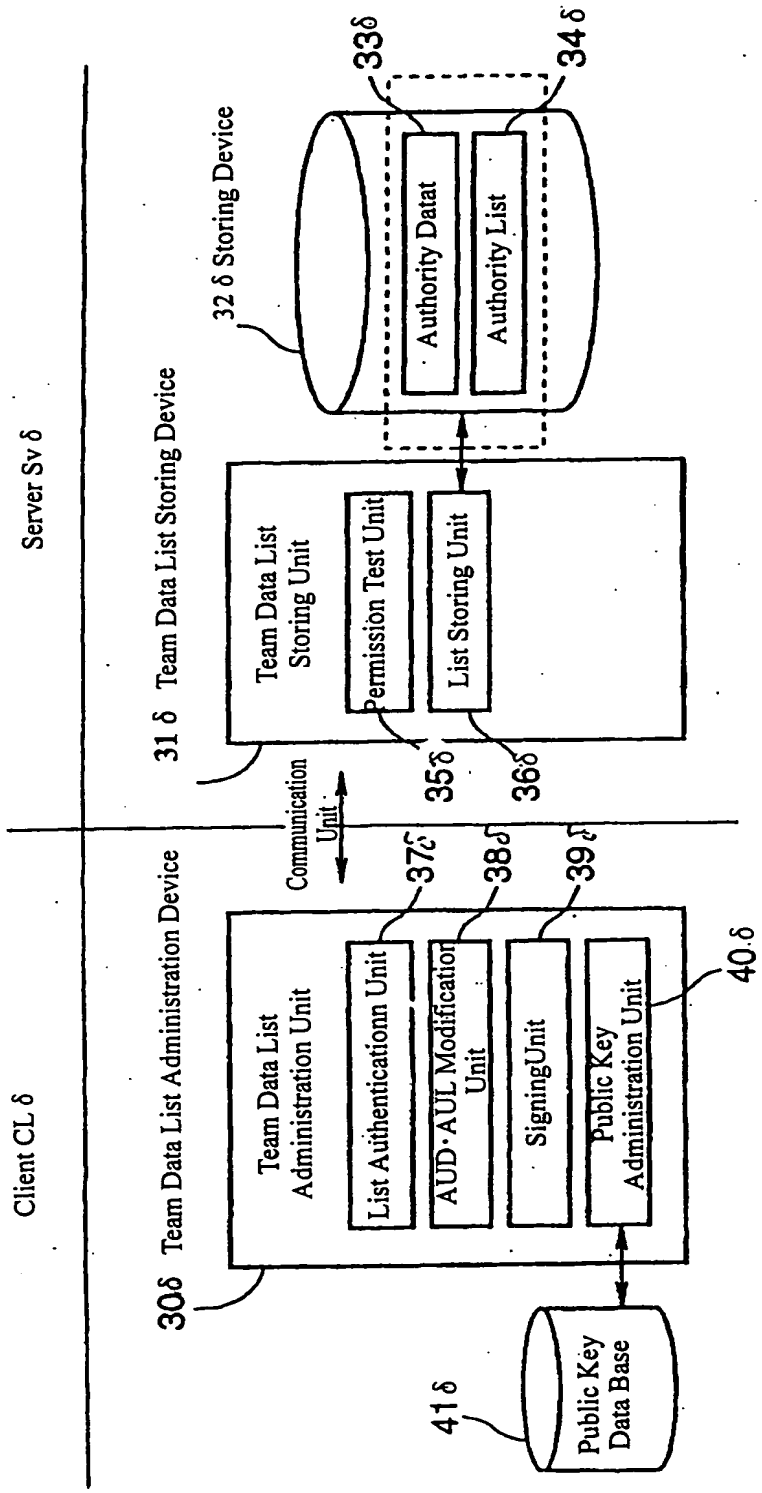

Information
Datapart 1
Datapart 2
Datapart 3
Datapart n
Encrypted Information
Encrypted Key 1
Encrypted Message 1
Encrypted Key 2
Encrypted Message 2
Encrypted Key 3
Encrypted Message 3
Digital Signature
Encrypted Key n
Encrypted Message n

FIG37


Client CL δ
Server Sv δ
Team Data List Administration Device
30δ
Team Data List Administration Unit
List Authentication Unit
AUD·AUL Modification Unit
SigningUnit
Public Key Administration Unit
40δ
37δ
38δ
39δ
Communication Unit
Team Data List Storing Device
31δ
Team Data List Storing Unit
Permission Test Unit
List Storing Unit
35δ
36δ
32δ Storing Device
Authority Datat
Authority List
33δ
34δ
41δ
Public Key Data Base

09700390 "070604

FIG38A

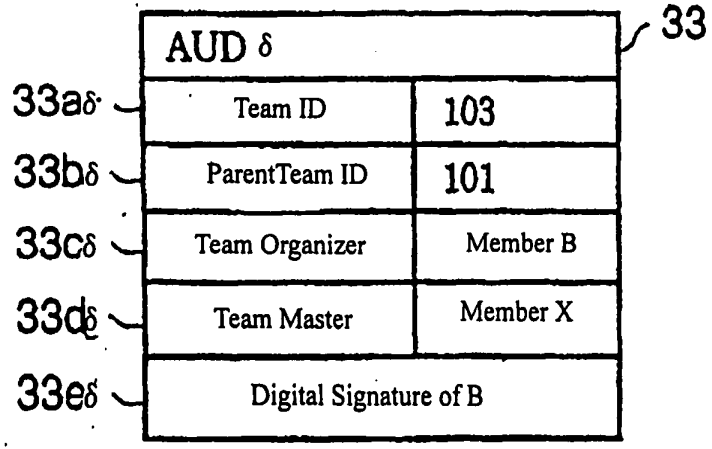


FIG38B

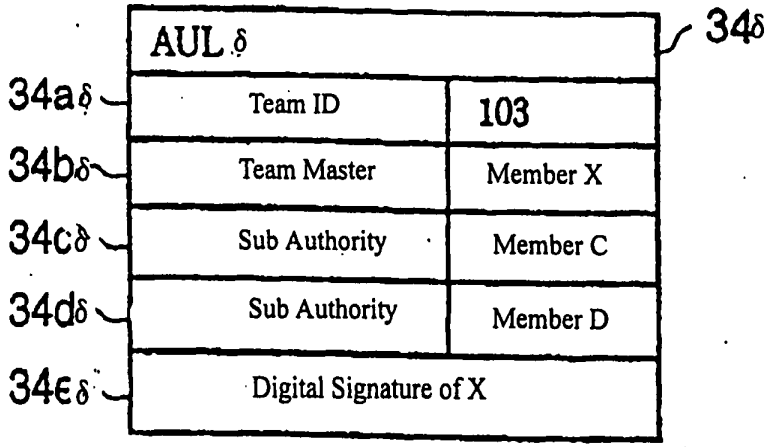


FIG38C

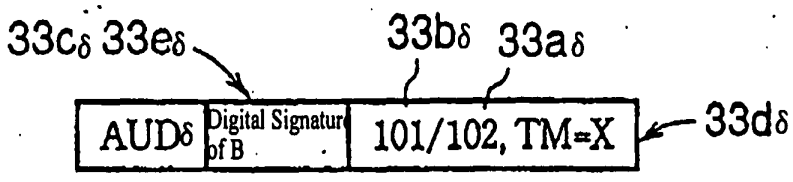
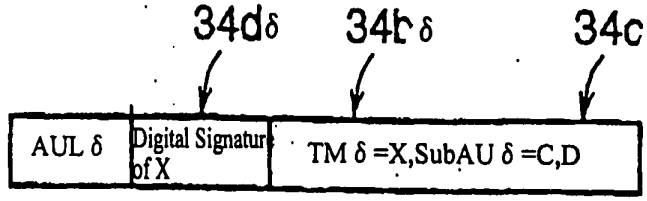
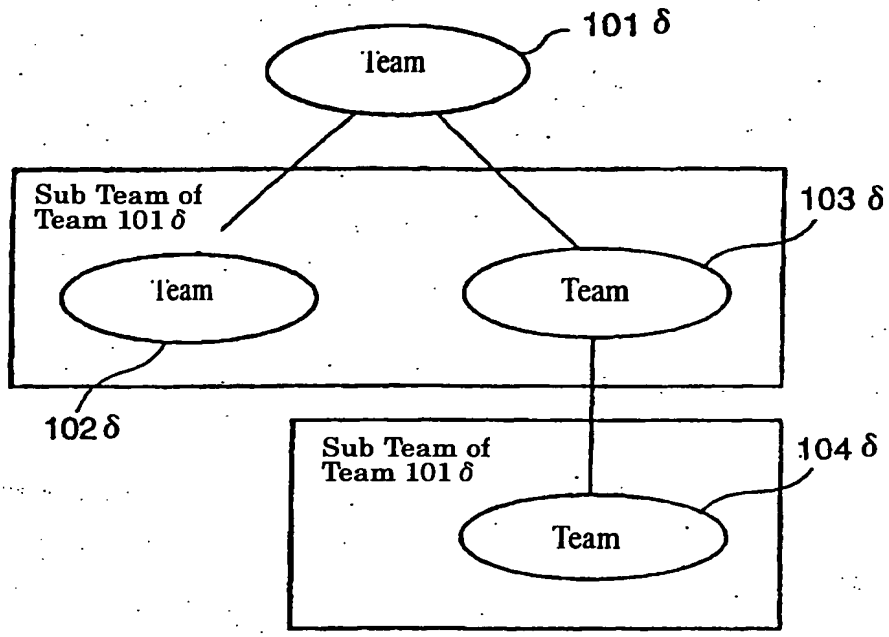


FIG38D



OBLON ET AL (703) 413-3000
DOCKET # 198041 US2PCT
SHEET 26 OF 73
09/700390

FIG.39


101 δ
Team
Sub Team of
Team 101 δ
103 δ
Team
Team
102 δ
Sub Team of
Team 101 δ
104 δ
Team

09/700390

T0940 " 05000540

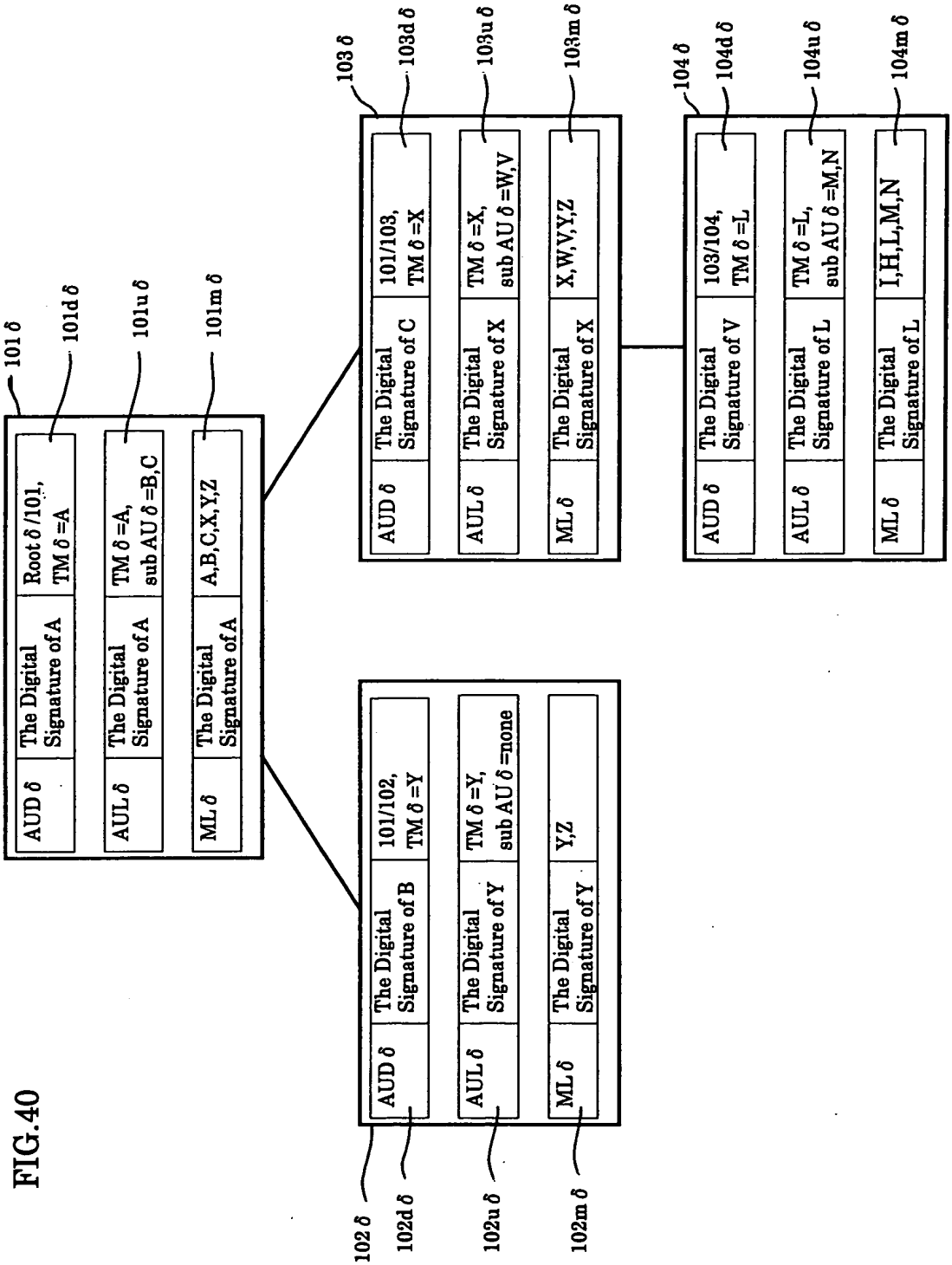
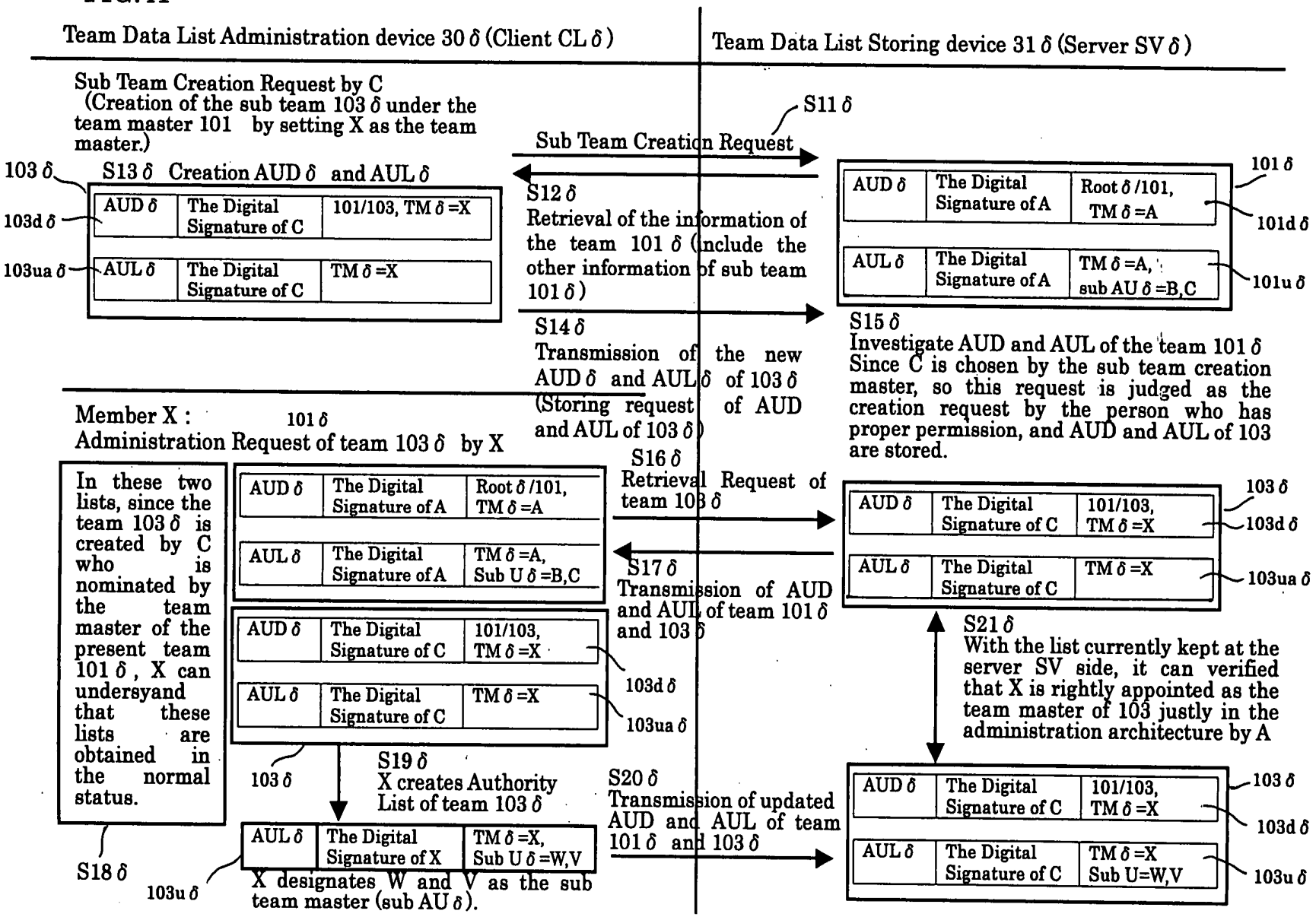


FIG.40

T090Z0"06E00Z60

FIG.41



OBLON ET AL (703) 413-3000
DOCKET # 1990118US01
SHEET 39 OF 73
09/700390

FIG.42

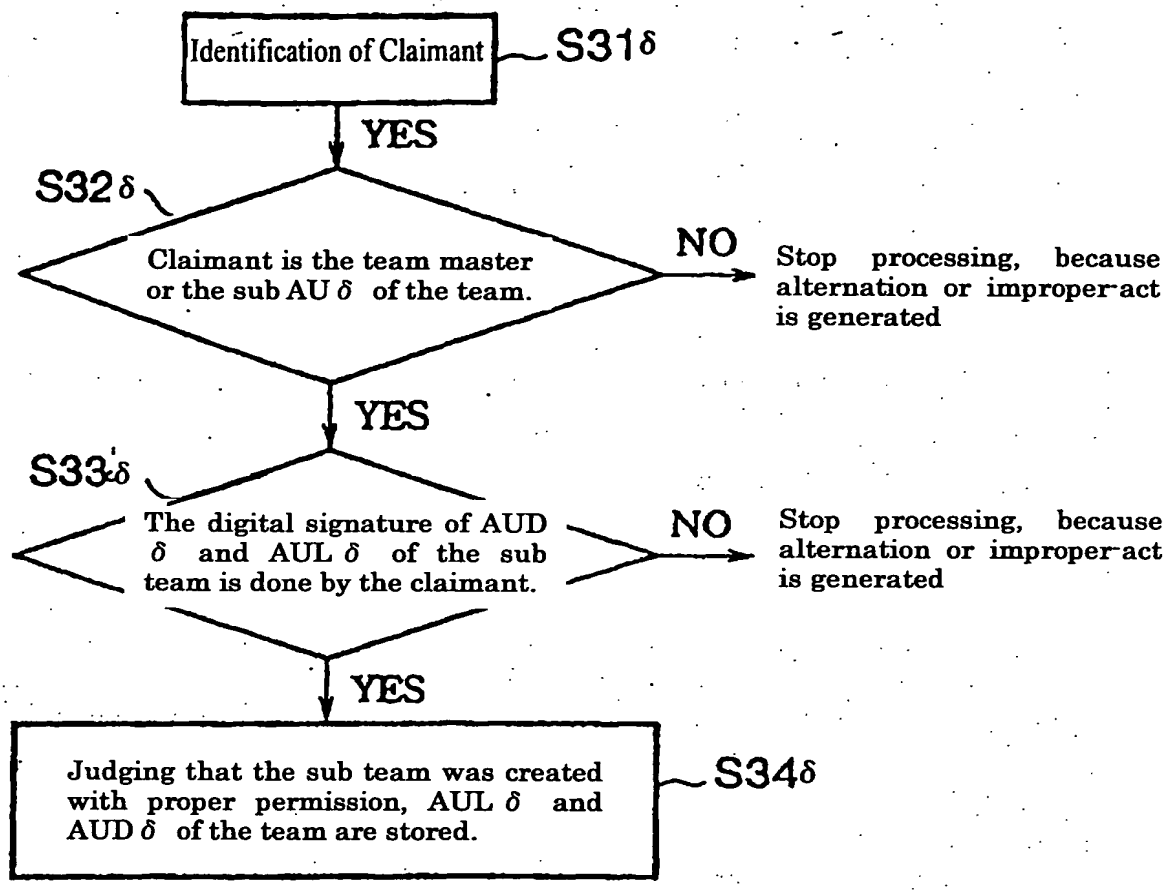

Identification of Claimant
S31δ
YES
S32δ
Claimant is the team master or the sub AU δ of the team.
NO
Stop processing, because alternation or improper-act is generated
YES
S33δ
The digital signature of AUD δ and AUL δ of the sub team is done by the claimant.
NO
Stop processing, because alternation or improper-act is generated
YES
Judging that the sub team was created with proper permission, AUL δ and AUD δ of the team are stored.
S34δ

FIG.43

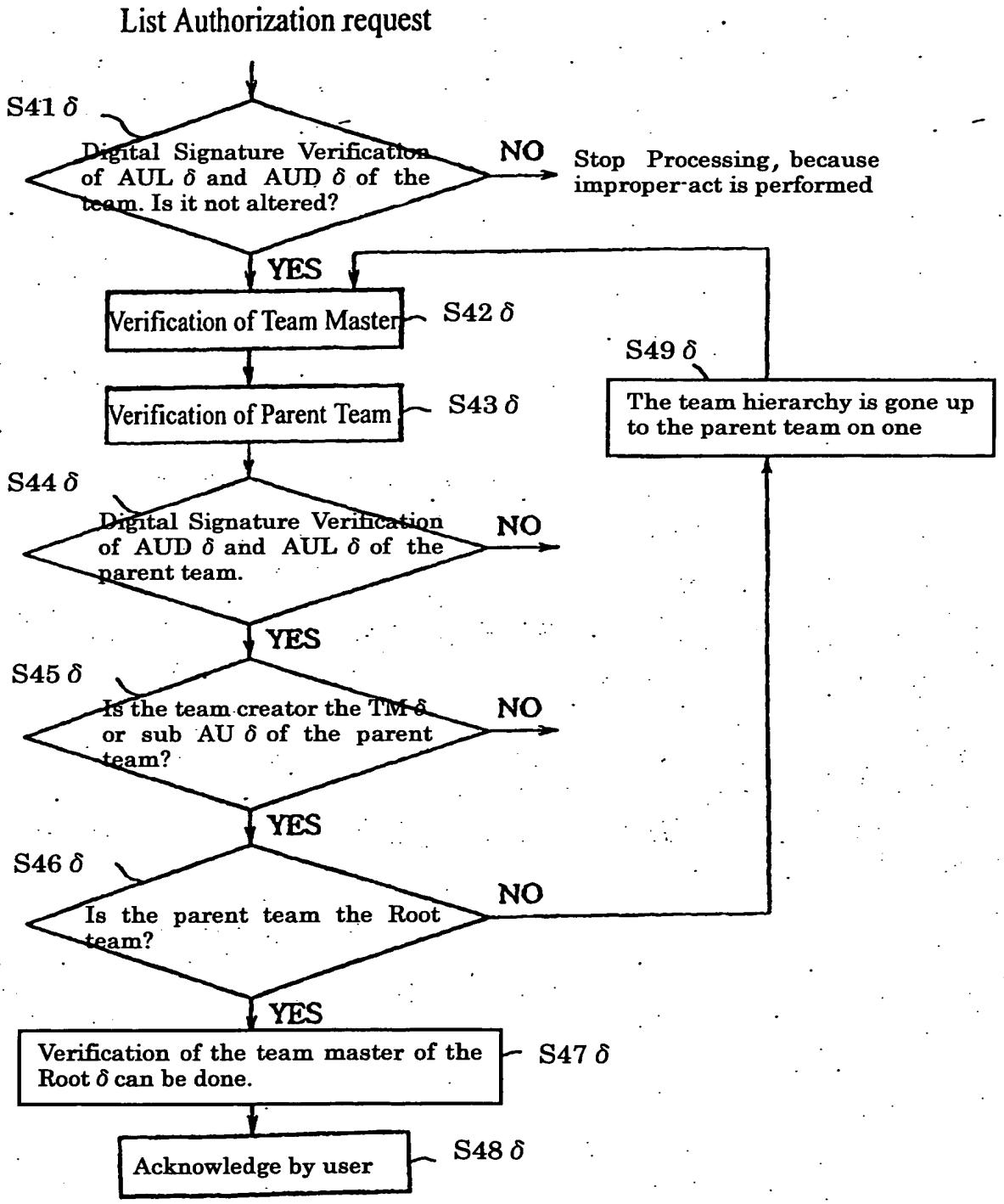

List Authorization request
S41 δ
Digital Signature Verification of AUL δ and AUD δ of the team. Is it not altered?
NO
Stop Processing, because improper act is performed
YES
Verification of Team Master
S42 δ
Verification of Parent Team
S43 δ
S44 δ
Digital Signature Verification of AUD δ and AUL δ of the parent team.
NO
YES
S45 δ
Is the team creator the TM δ or sub AU δ of the parent team?
NO
YES
S46 δ
Is the parent team the Root team?
NO
YES
S49 δ
The team hierarchy is gone up to the parent team on one
Verification of the team master of the Root δ can be done.
S47 δ
Acknowledge by user
S48 δ

FIG.44

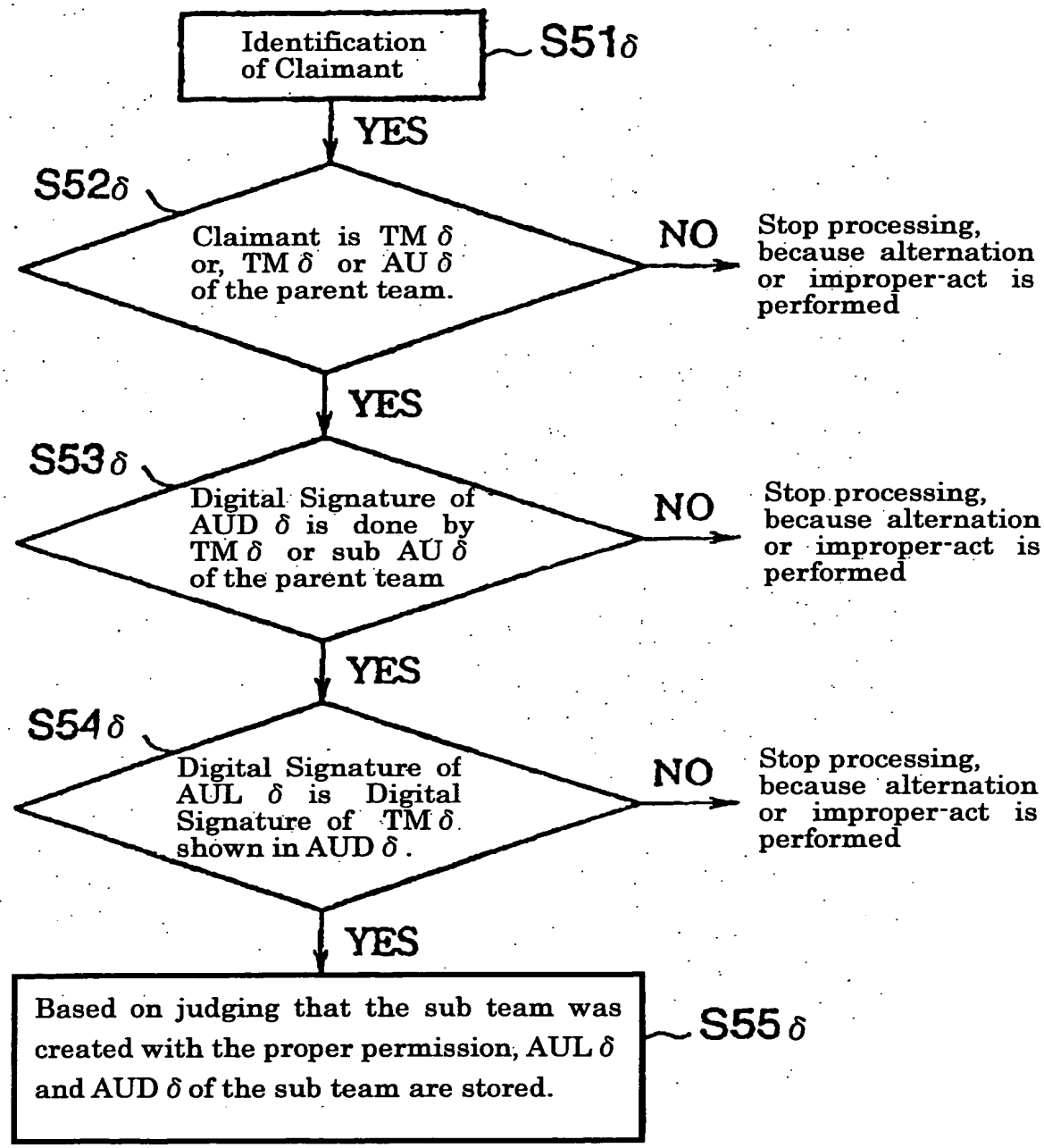
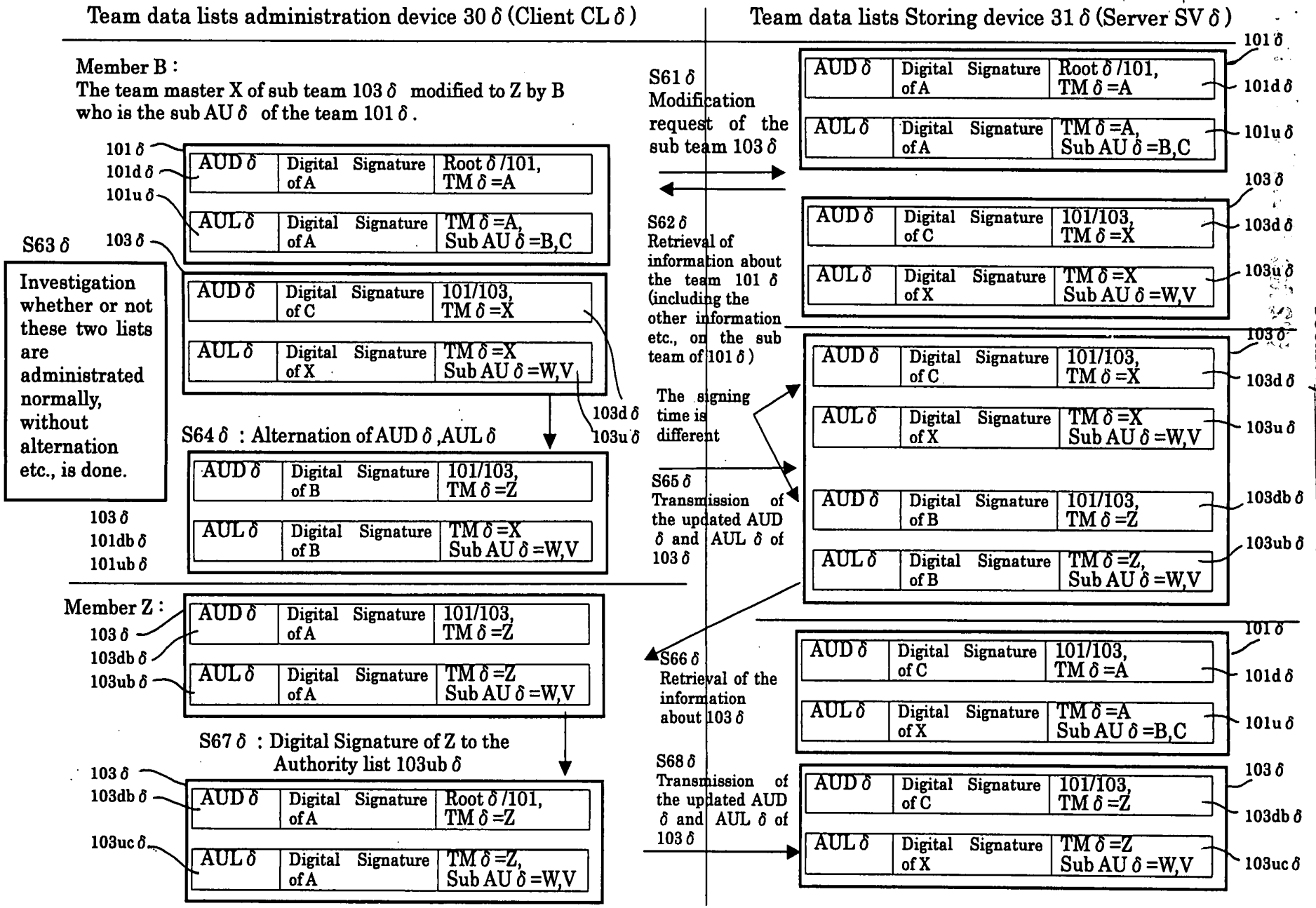

Identification of Claimant
S51δ
YES
S52δ
Claimant is TM δ or, TM δ or AU δ of the parent team.
NO
Stop processing, because alternation or improper-act is performed
YES
S53δ
Digital Signature of AUD δ is done by TM δ or sub AU δ of the parent team
NO
Stop processing, because alternation or improper-act is performed
YES
S54δ
Digital Signature of AUL δ is Digital Signature of TM δ shown in AUD δ.
NO
Stop processing, because alternation or improper-act is performed
YES
Based on judging that the sub team was created with the proper permission, AUL δ and AUD δ of the sub team are stored.
S55δ

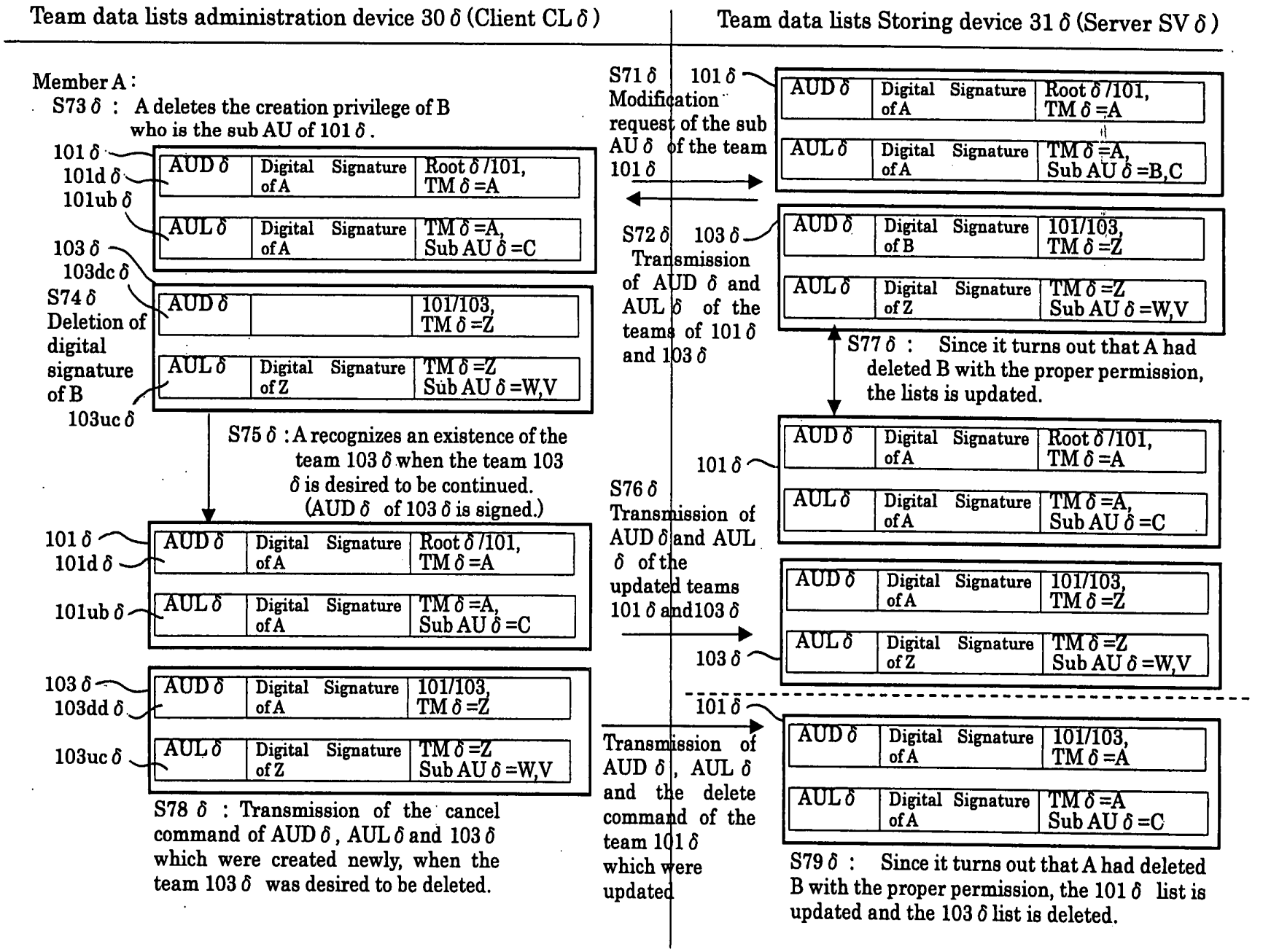
FIG.45



OBLON ET AL (703) 413-3000
DOCKET # 149101US2
SHEET 43 OF

T09070 06E00760

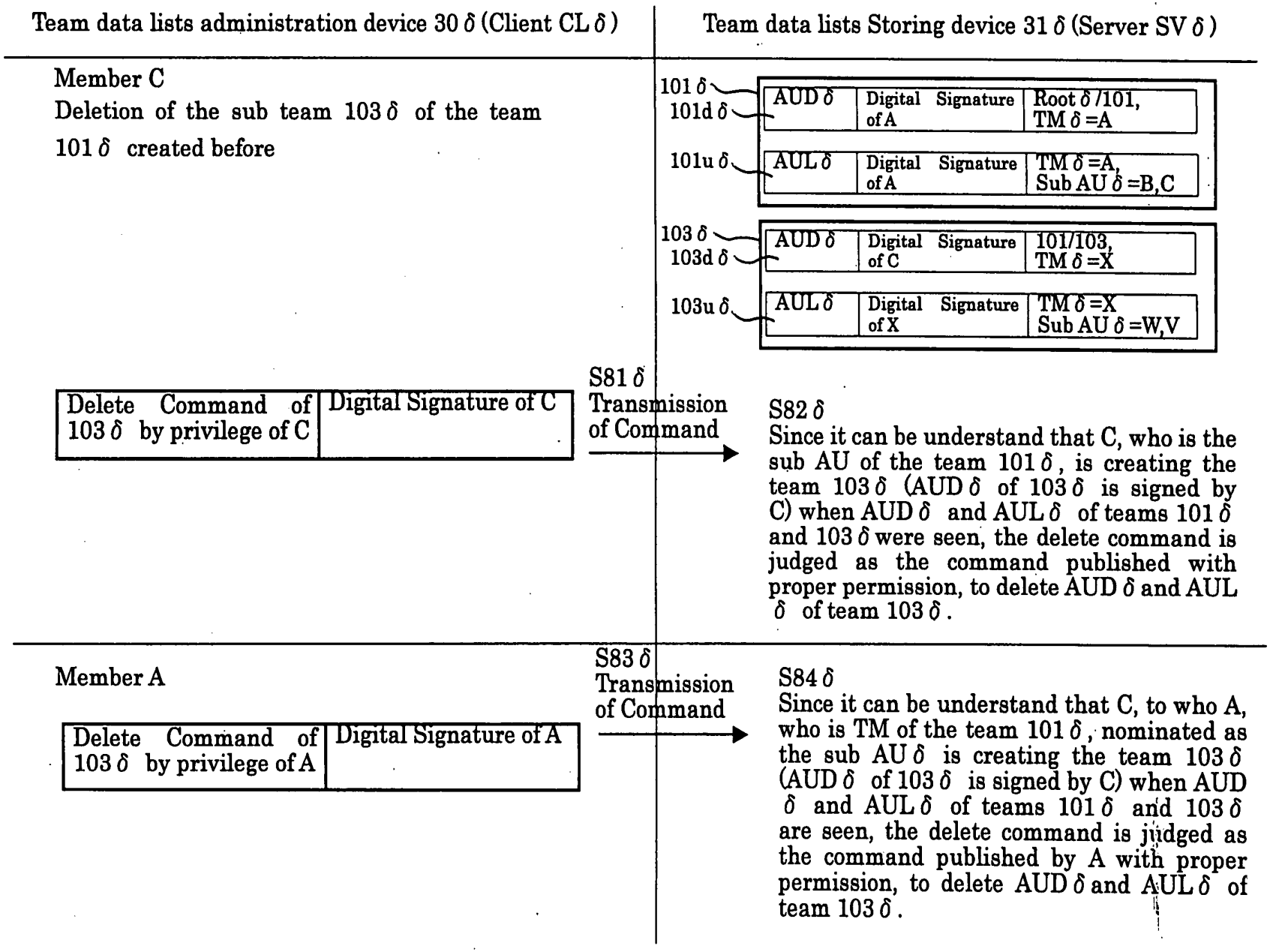
FIG.46



OBLON ET AL (703) 413-3000
DOCKET # 1990.41 US2 Cr
SHEET 44 OF 72
09/700390

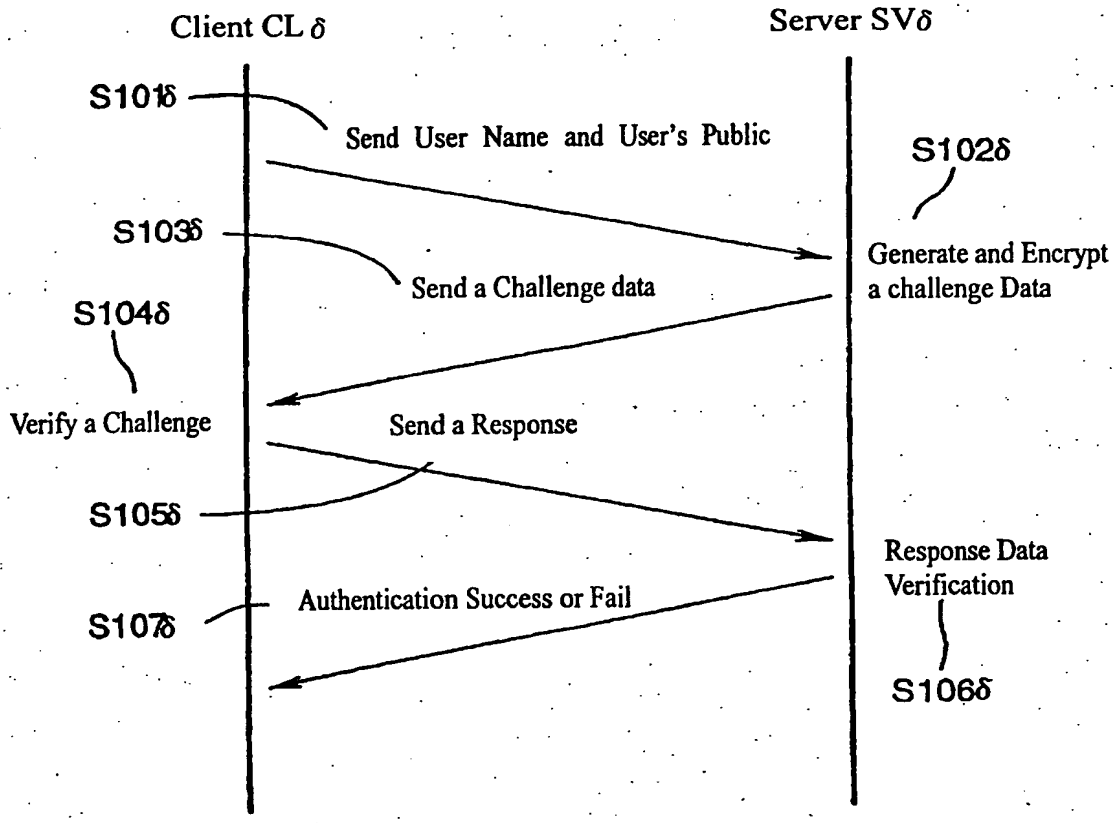
T090Z0" 06E00Z60

FIG.47



OBLON ET AL (703) 413-3000
DOCKET #
SHEET 45 OF 47
09/700390

FIG.48


Client CL δ
Server SVδ
S101δ
Send User Name and User's Public
S102δ
S103δ
Send a Challenge data
Generate and Encrypt a challenge Data
S104δ
Verify a Challenge
Send a Response
S105δ
Response Data Verification
Authentication Success or Fail
S107δ
S106δ

T0940 "06040

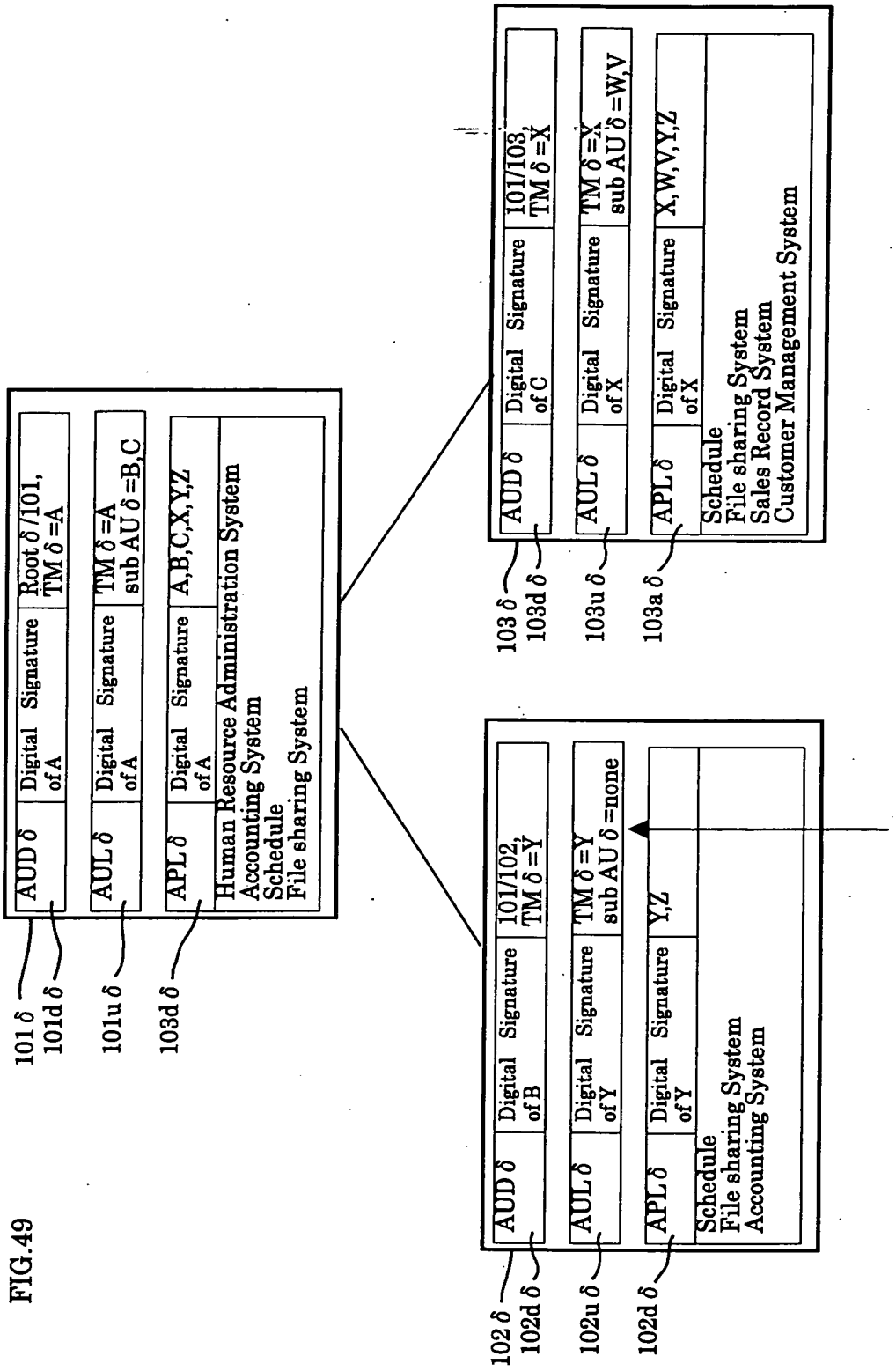


FIG.49

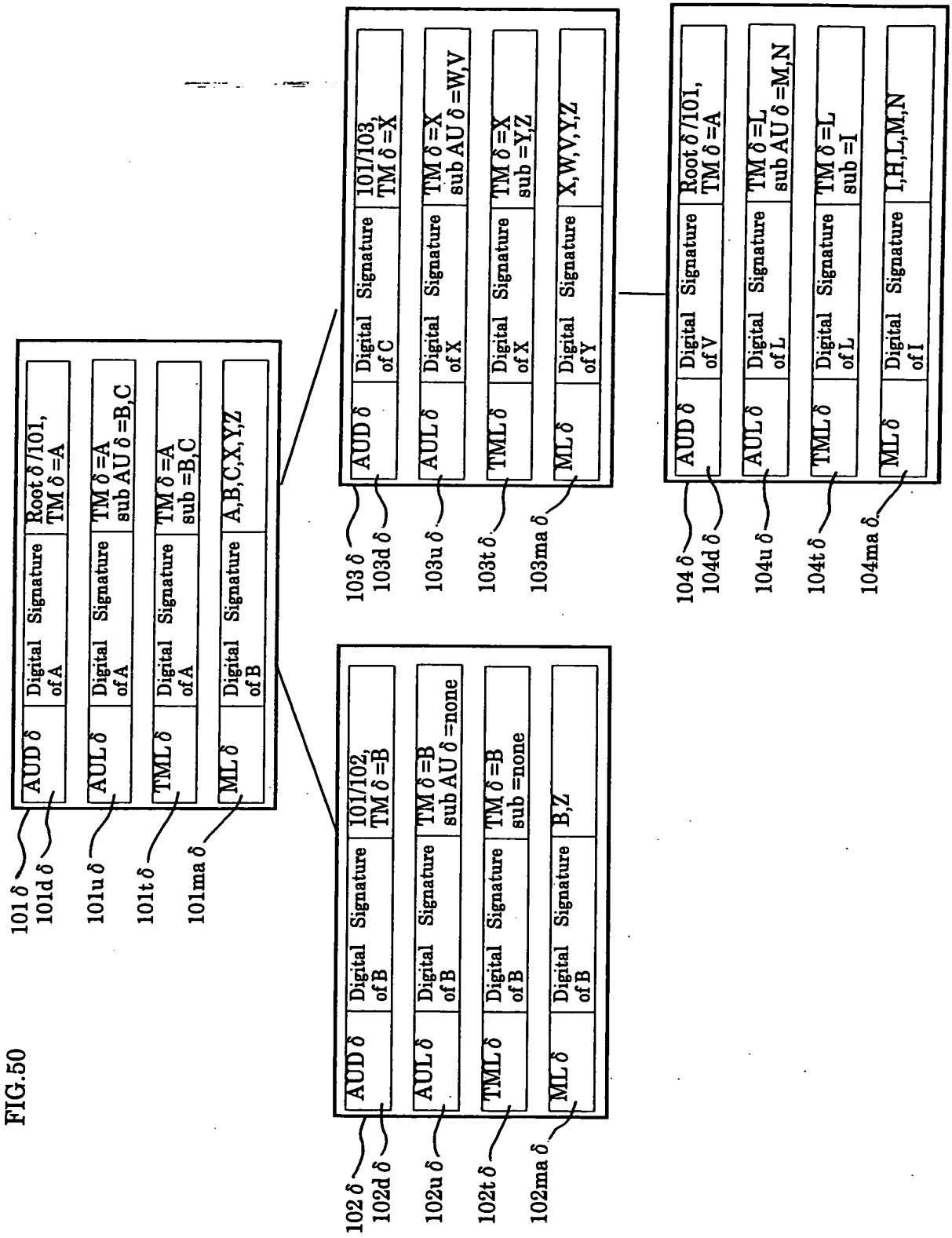
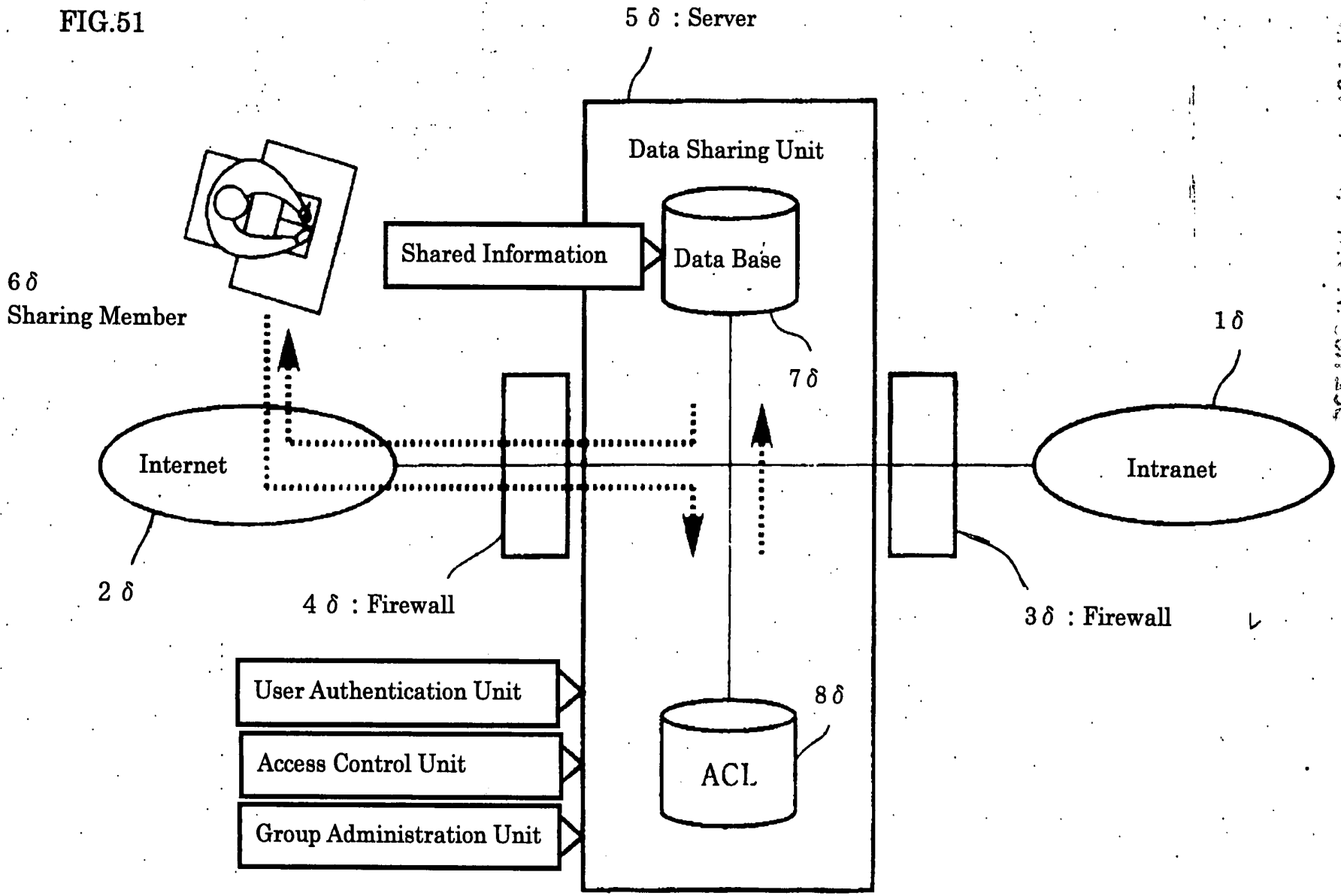


FIG.50

T0960 "060260

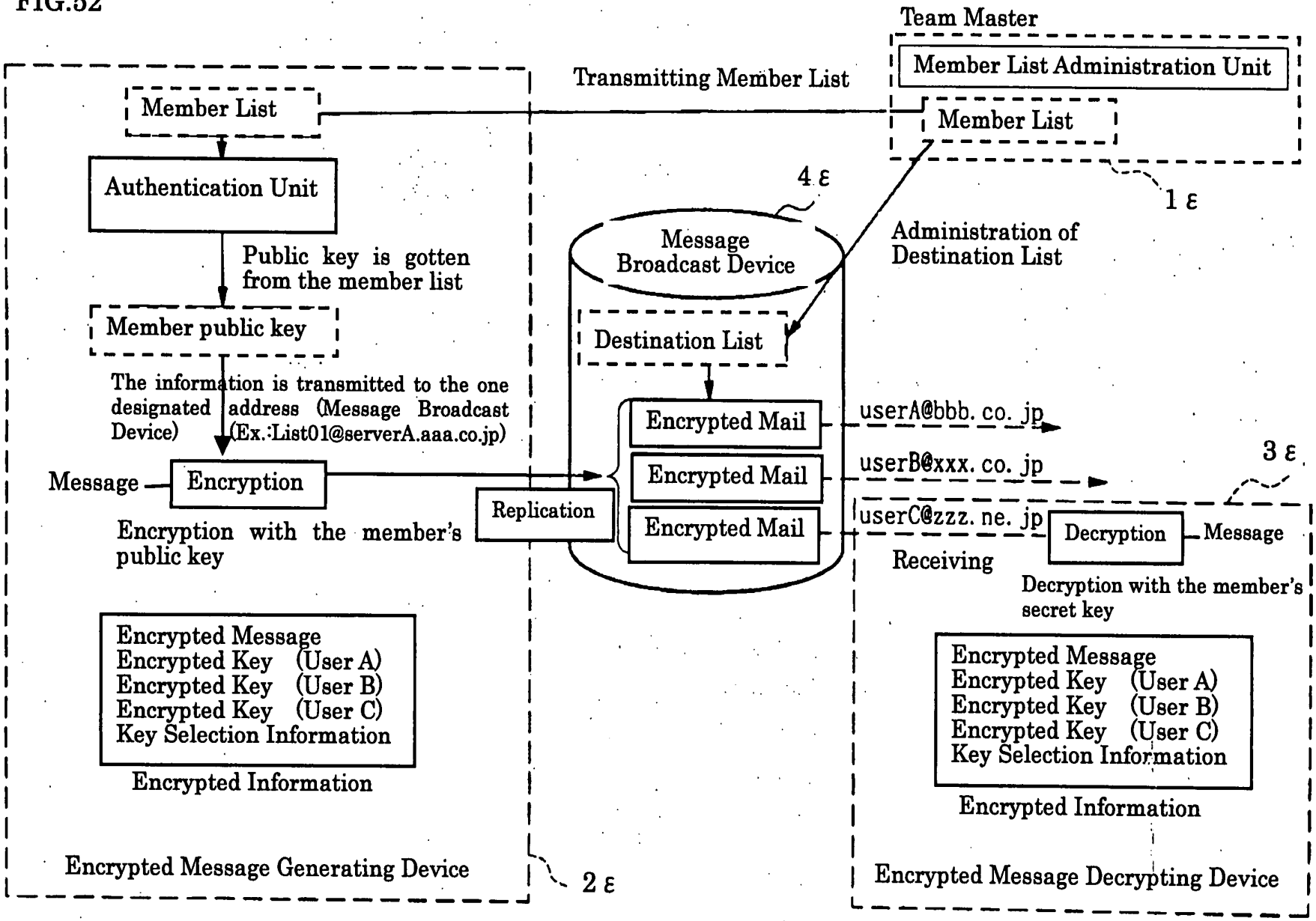
FIG.51



OBLON ET AL (703) 413-3000
DOCKET # 1946US96
SHEET 40 OF
09/700390

T09020"06E00760

FIG.52



OBLON ET AL (703) 413-3000
DOCKET # MAT-8157
SHEET 52 OF 71
09/700390

FIG.53

Member List

Team 101 ε
Member-X
Member-Y : Member-B
Digital Signature of X

FIG.54

Team Master List

Team 101 ε	
Member-X	Master
Member-Y	Sub
Member-Z	Sub
Digital Signature of X	

Member List

Team 101 ε
Member-X
Member-Y : Member-B
Digital Signature of X

09700390 "0070001

FIG.55

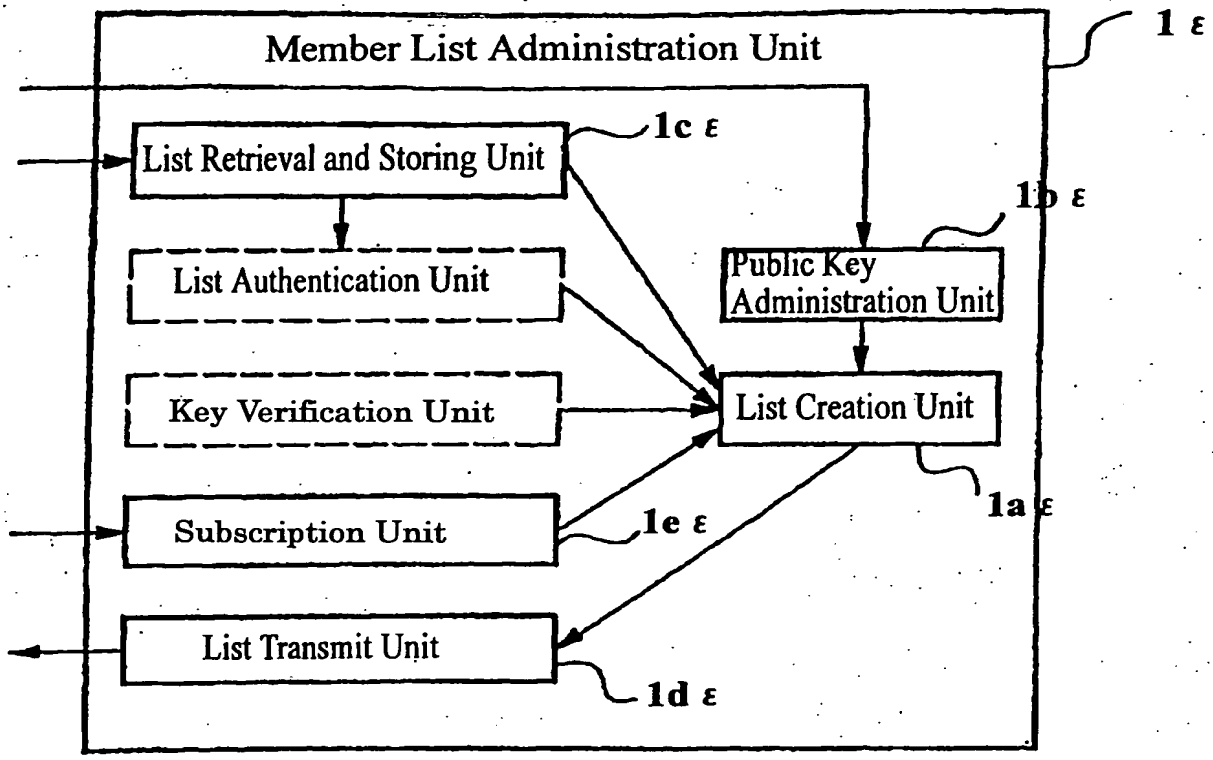

Member List Administration Unit
1 ε
List Retrieval and Storing Unit
1c ε
List Authentication Unit
Public Key Administration Unit
1b ε
Key Verification Unit
List Creation Unit
1a ε
Subscription Unit
1e ε
List Transmit Unit
1d ε

FIG.56

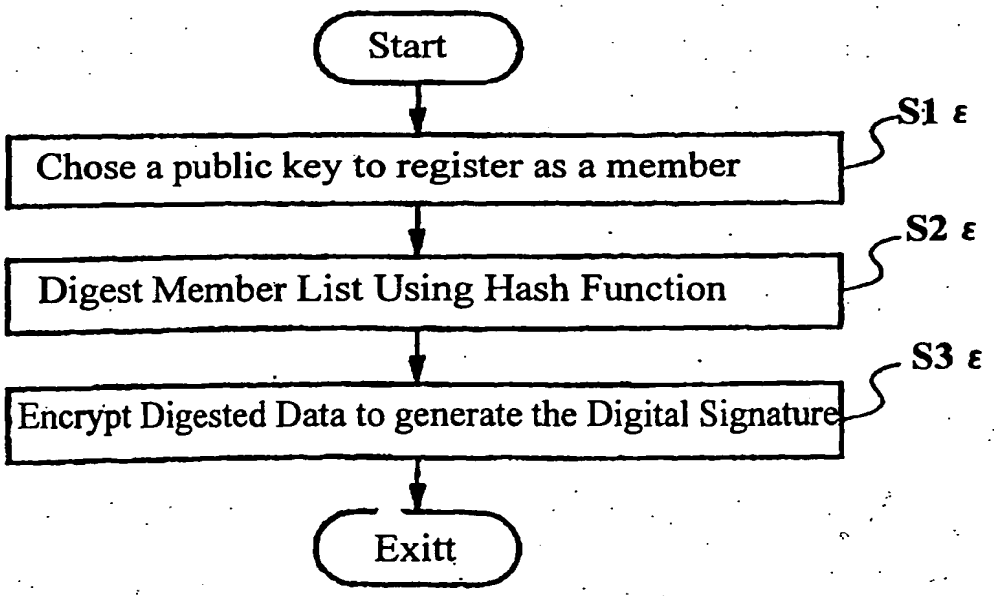
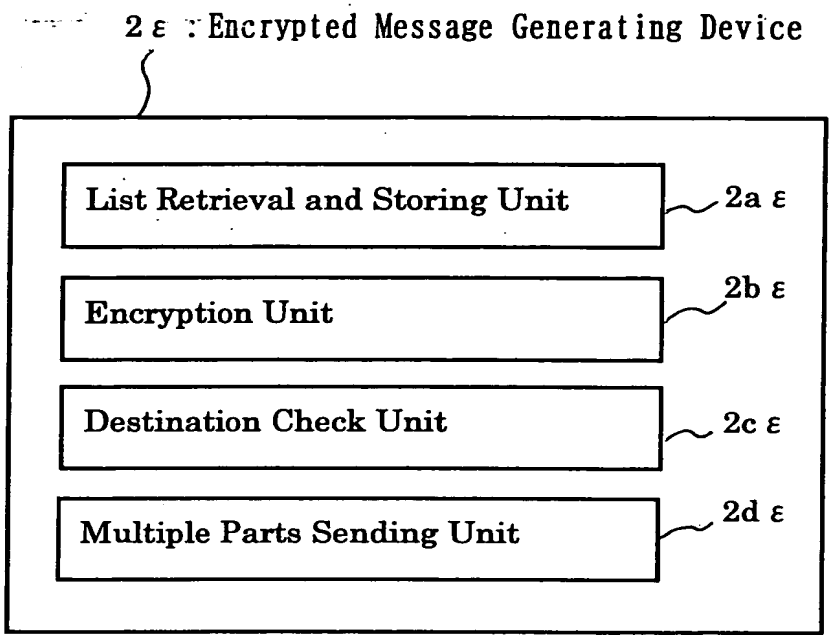

Start
Chose a public key to register as a member
S1 ε
Digest Member List Using Hash Function
S2 ε
Encrypt Digested Data to generate the Digital Signature
S3 ε
Exitt

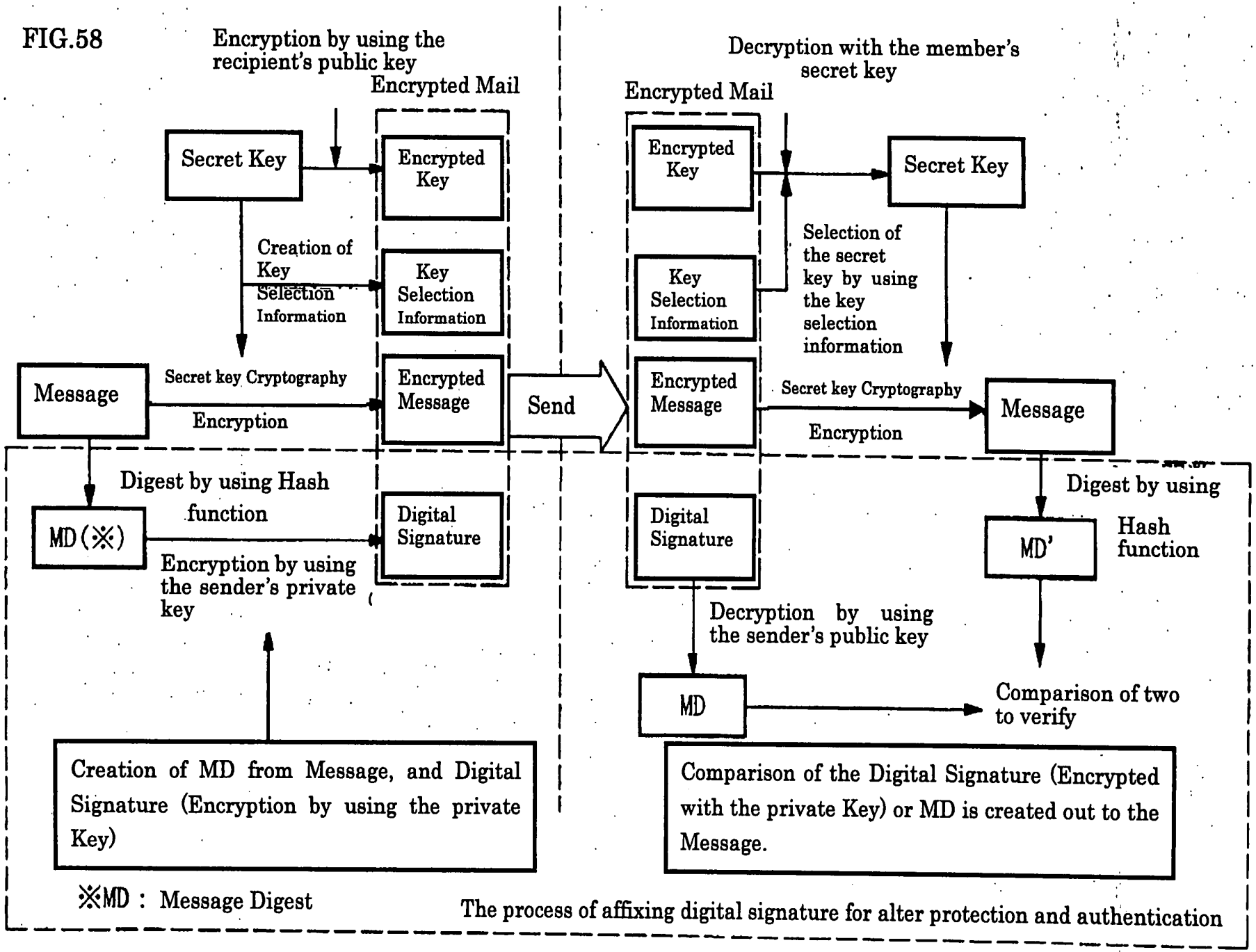
FIG.57



09/700390 05/00/2001

T0902 0 06E0026D

FIG.58



OBLON ET AL (703) 413-3000
DOCKET # 1981US00
SHEET 54 OF 72
09/700390

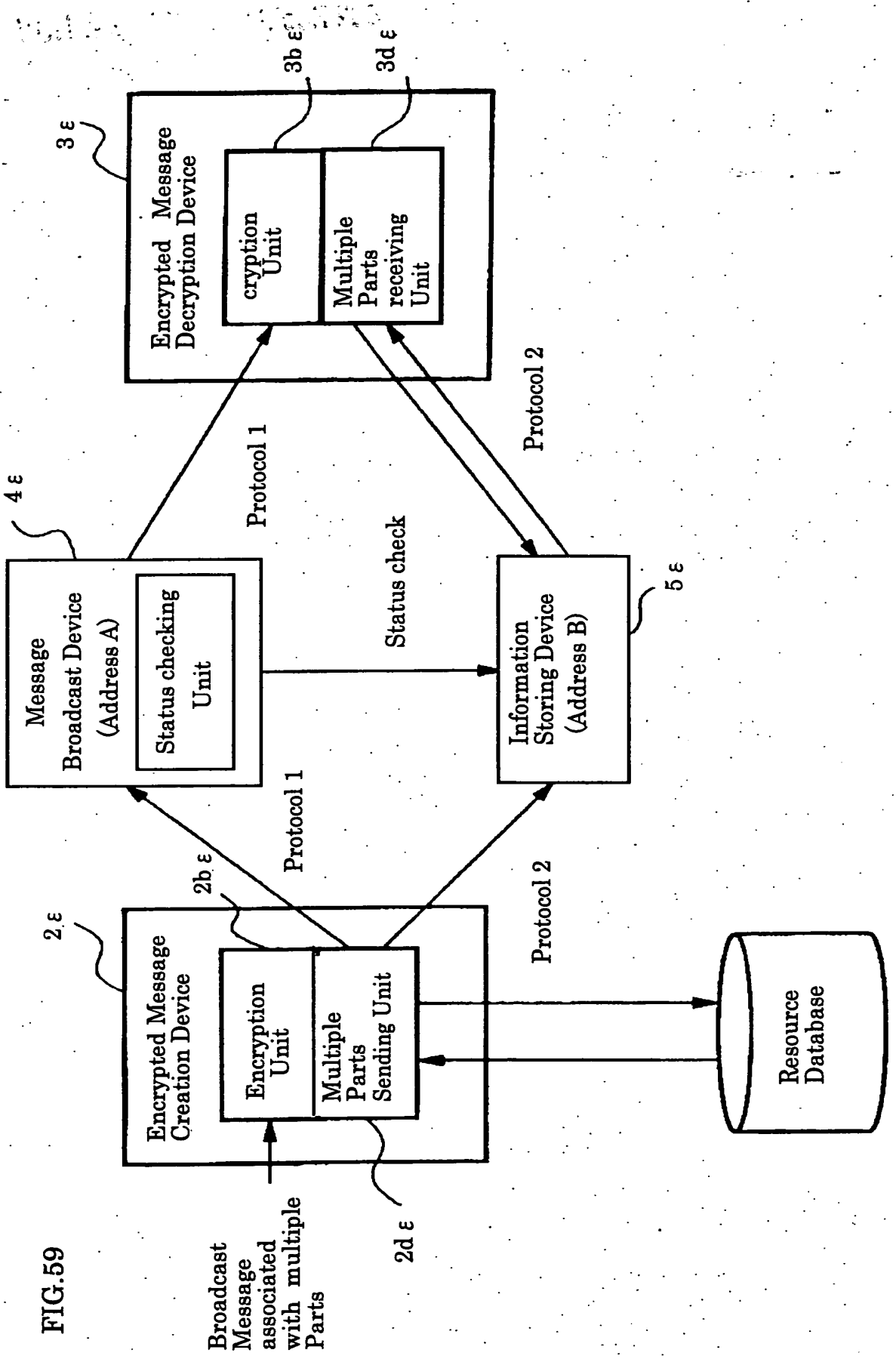
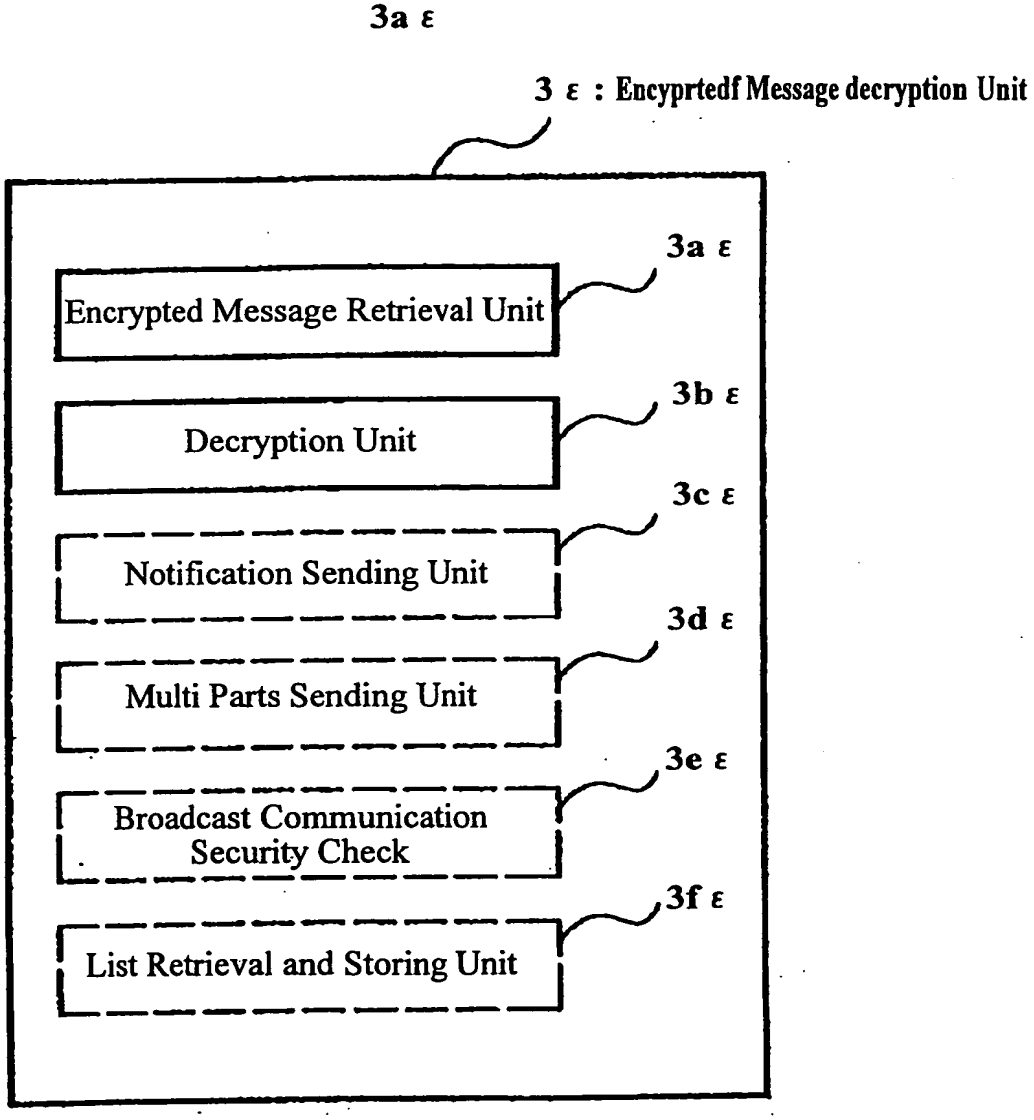

Broadcast Message associated with multiple Parts
2 ε
Encrypted Message Creation Device
2b ε
Encryption Unit
Multiple Parts Sending Unit
2d ε
Protocol 1
Protocol 2
Message Broadcast Device (Address A)
4 ε
Status checking Unit
Status check
Information Storing Device (Address B)
5 ε
Resource Database
3 ε
Encrypted Message Decryption Device
3b ε
cryption Unit
3d ε
Multiple Parts receiving Unit
Protocol 1
Protocol 2

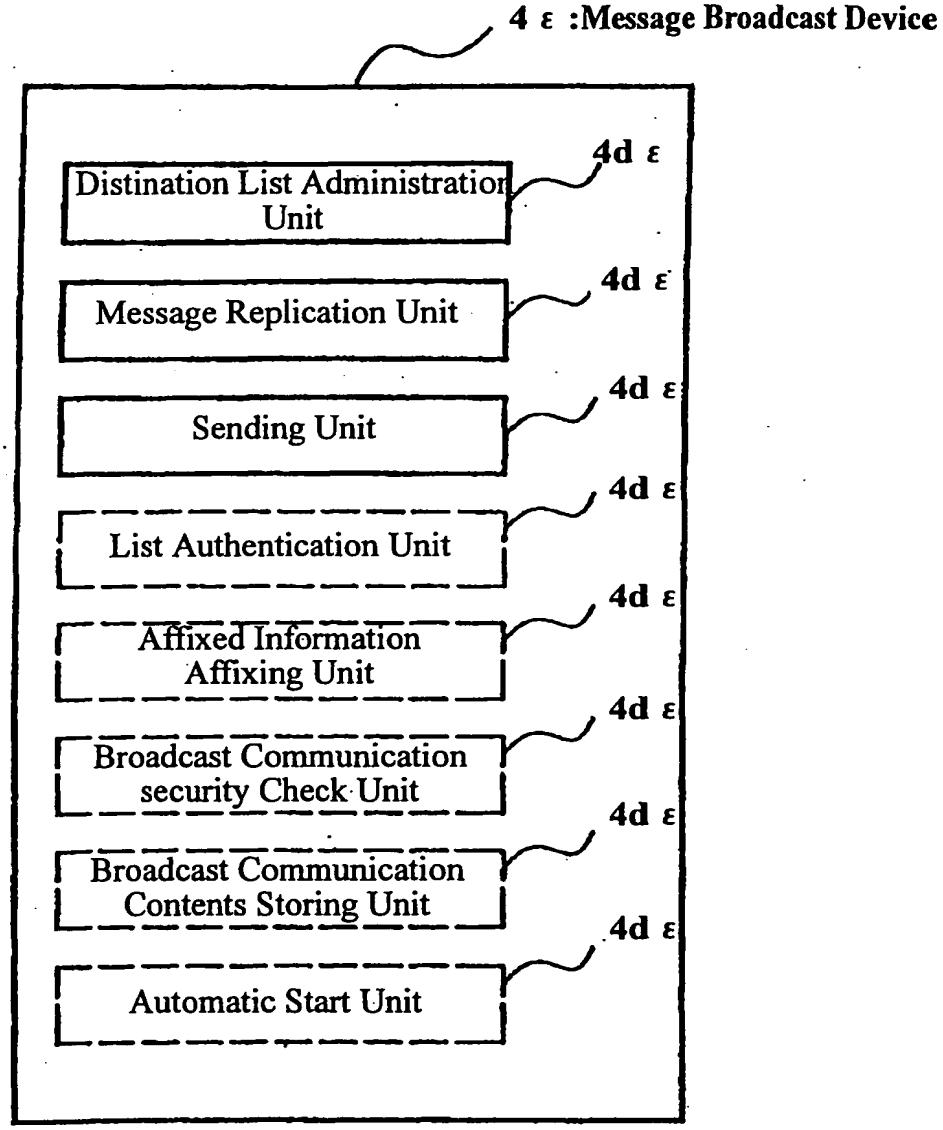
FIG.59

FIG.60



T09040 "050300450

FIG.61


4 ε :Message Broadcast Device
Distination List Administration Unit
4d ε
Message Replication Unit
4d ε
Sending Unit
4d ε
List Authentication Unit
4d ε
Affixed Information Affixing Unit
4d ε
Broadcast Communication security Check Unit
4d ε
Broadcast Communication Contents Storing Unit
4d ε
Automatic Start Unit
4d ε

OBLON ET AL (703) 413-3000
DOCKET # 1996911US2IG SHEET 58 OF 73

"09700390"

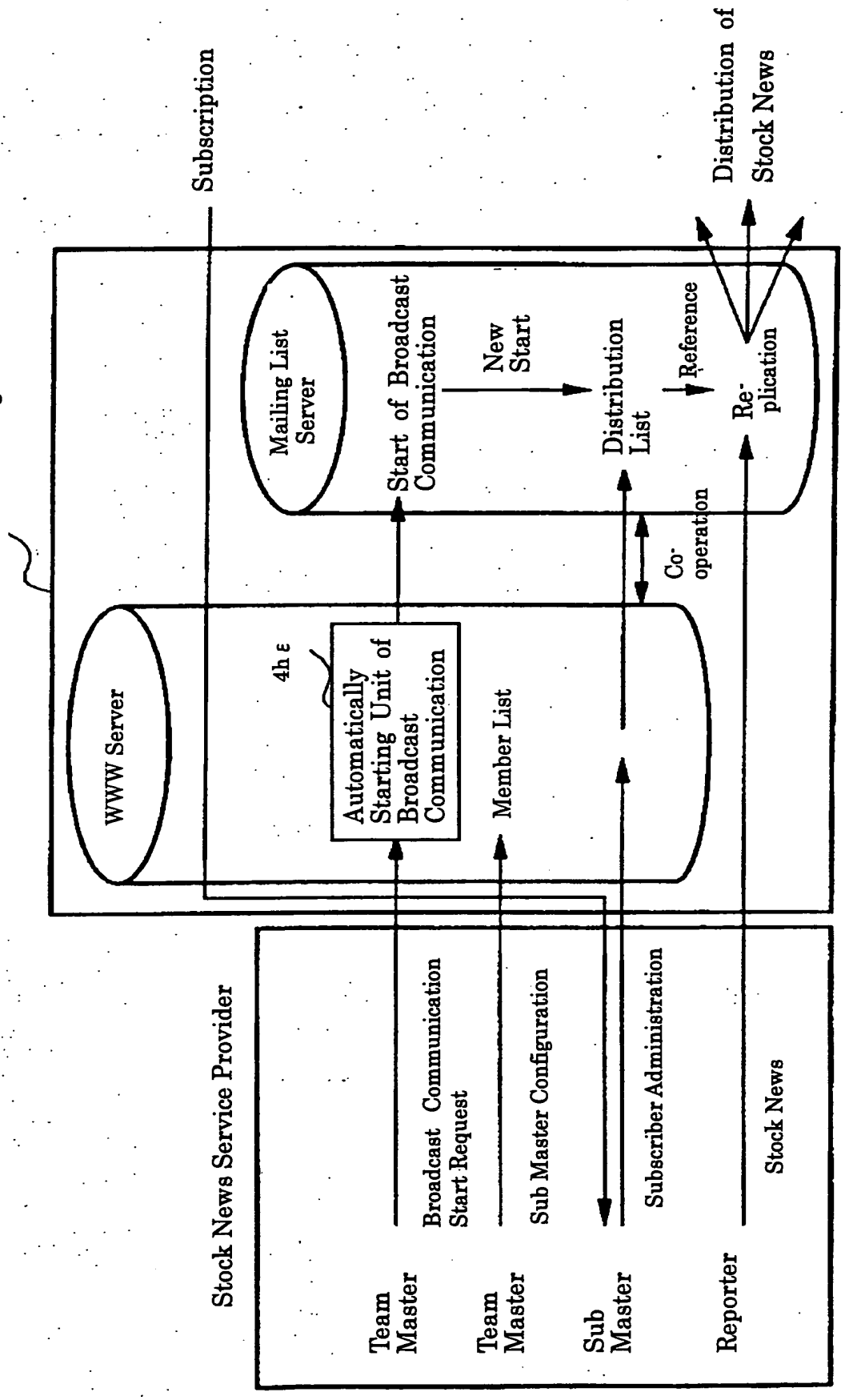
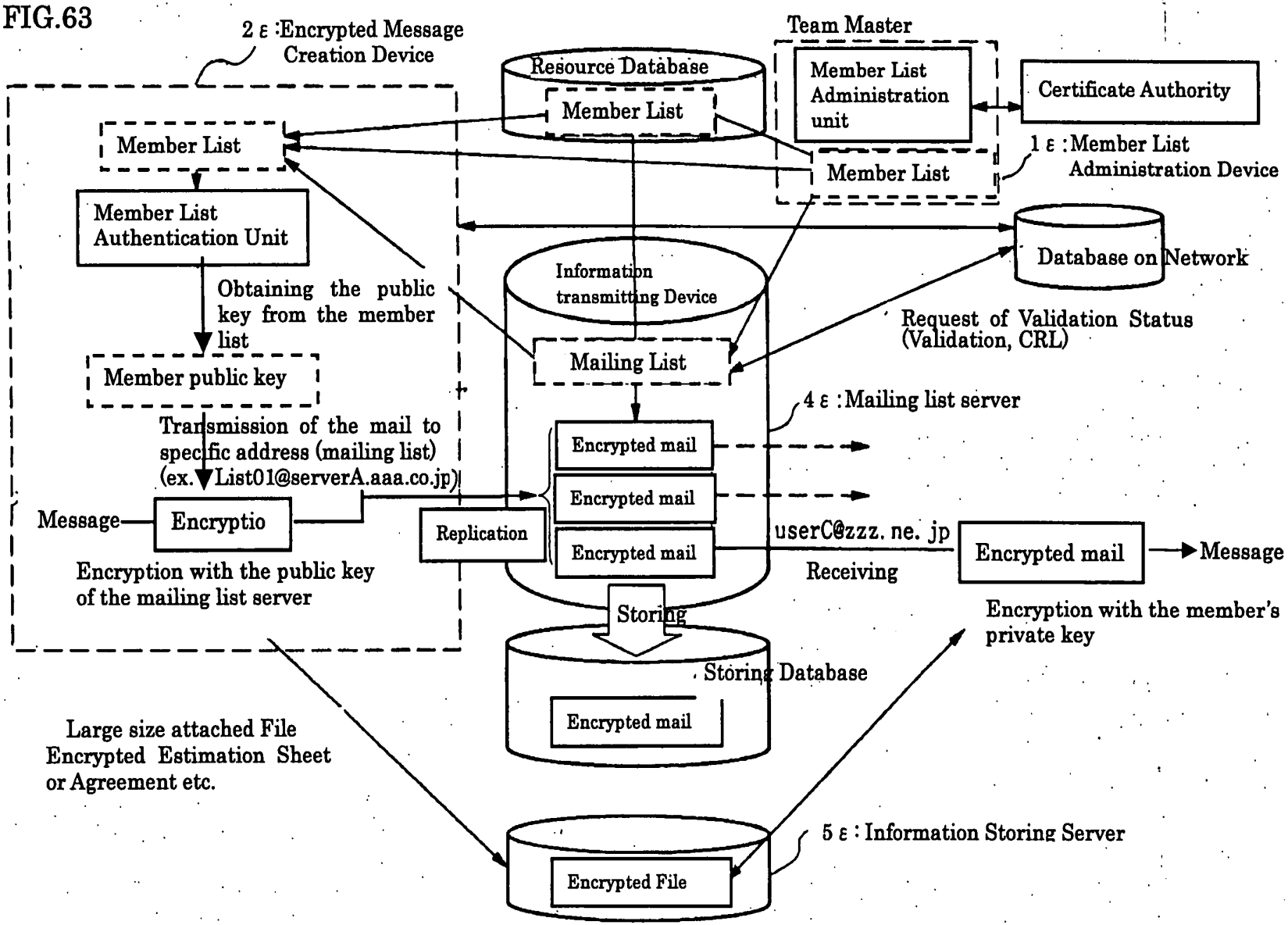


FIG.62

T09070 06E002G0

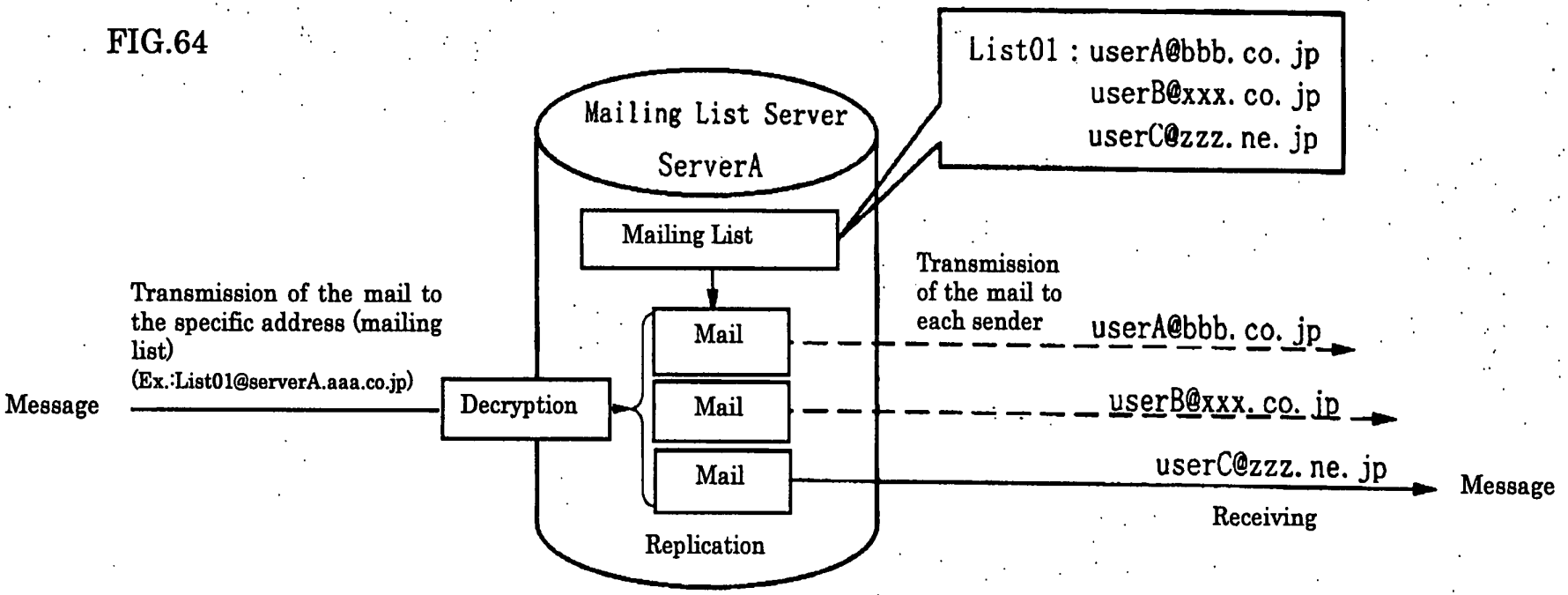
FIG.63



OBLON ET AL (703) 413-3000
DOCKET # 1946US02B
SHEET 13 OF 13
09/700390

09700390 "070604

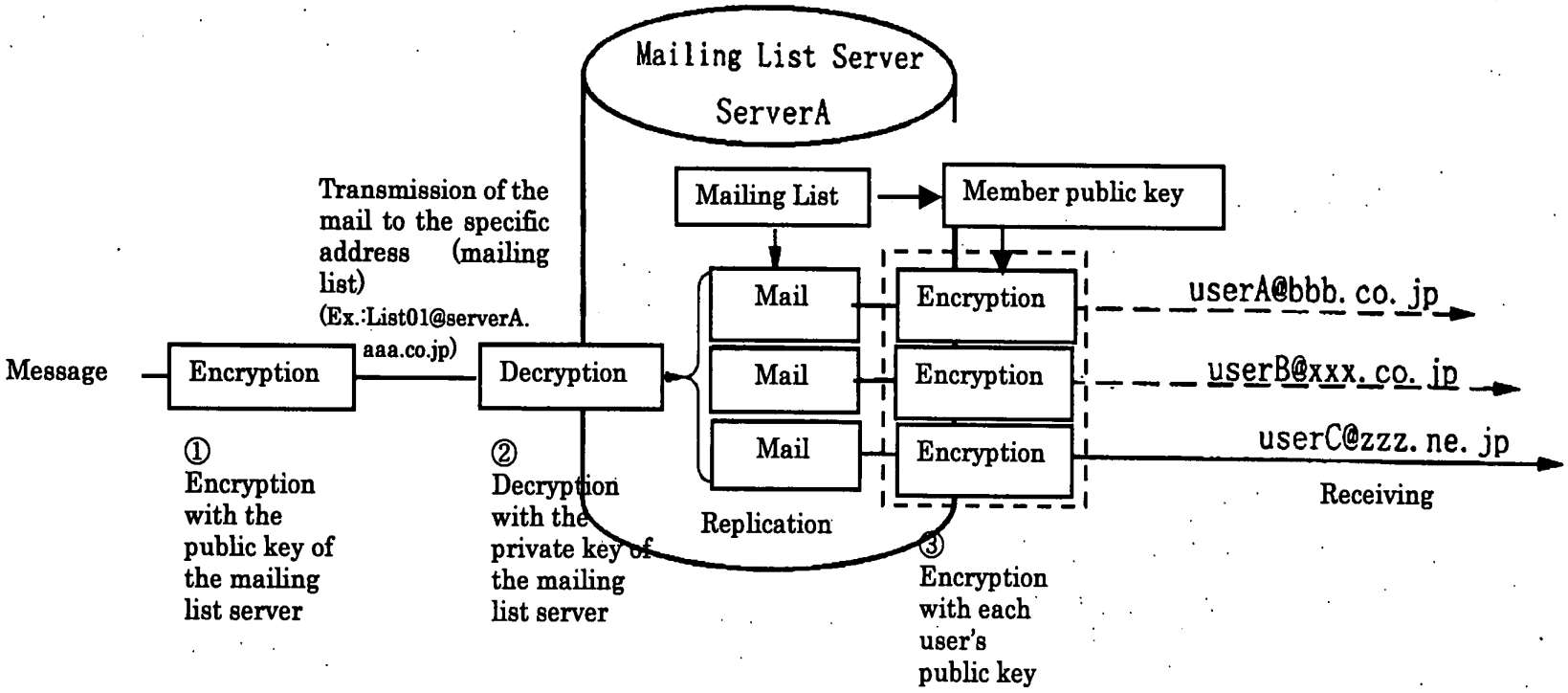
FIG.64



OBLON ET AL (703) 413-3000
DOCKET #
SHEET 60 OF 73
09/700390

T09070 "06E00760

FIG.65



OBLON ET AL (703) 413-3000
DOCKET # 9419 US 2PCT SHEET 41 OF 73
09/700390

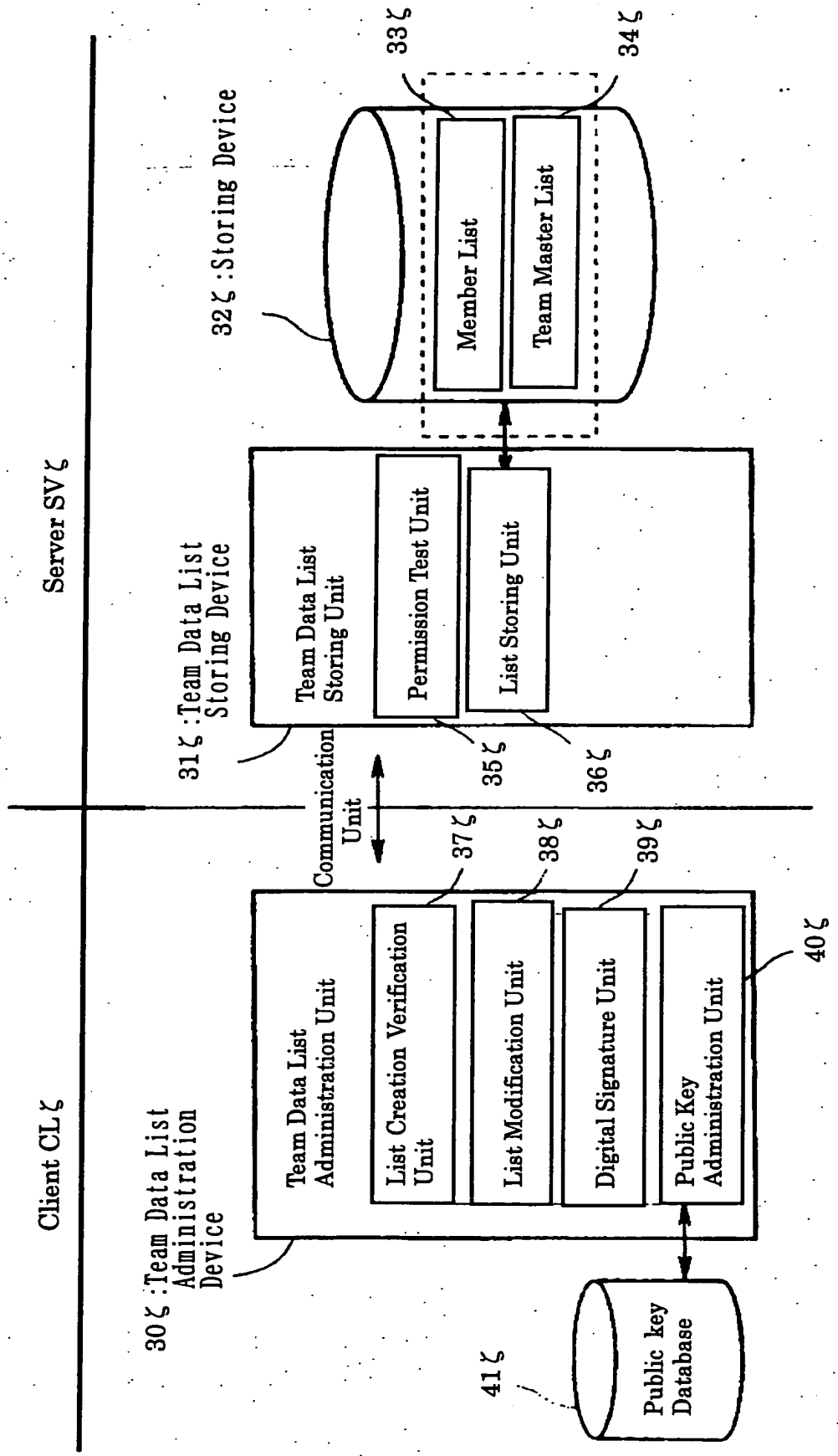
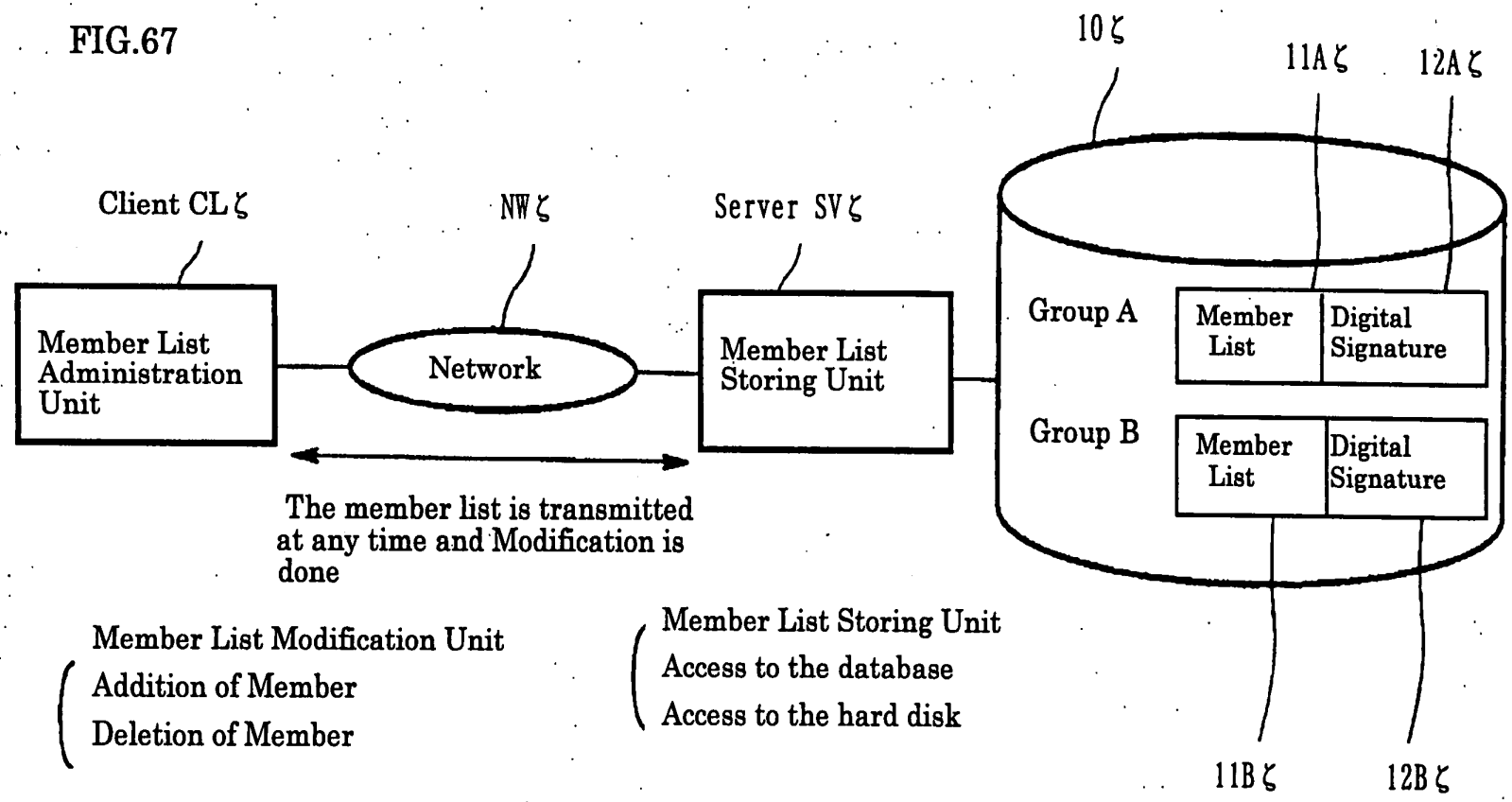

Server SV ζ
Client CL ζ
33 ζ
34 ζ
32 ζ :Storing Device
Member List
Team Master List
31 ζ :Team Data List Storing Device
Team Data List Storing Unit
Permission Test Unit
List Storing Unit
35 ζ
36 ζ
Communication Unit
37 ζ
38 ζ
39 ζ
40 ζ
30 ζ :Team Data List Administration Device
Team Data List Administration Unit
List Creation Verification Unit
List Modification Unit
Digital Signature Unit
Public Key Administration Unit
41 ζ
Public key Database

FIG.66

T09070 "06E00760

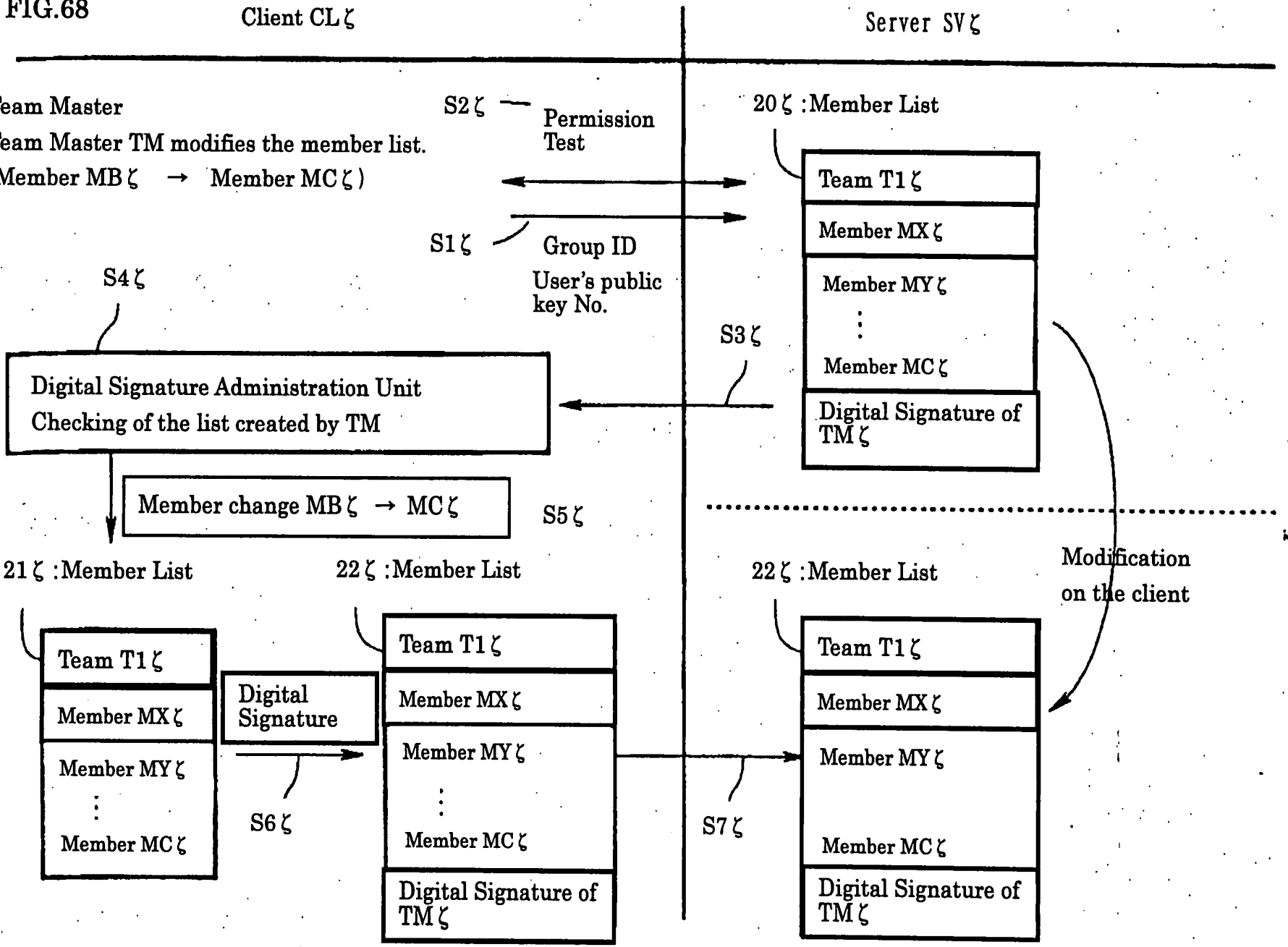
FIG.67



OBLON ET AL (703) 413-3000
DOCKET #
SHEET 13 OF 13
09/700390

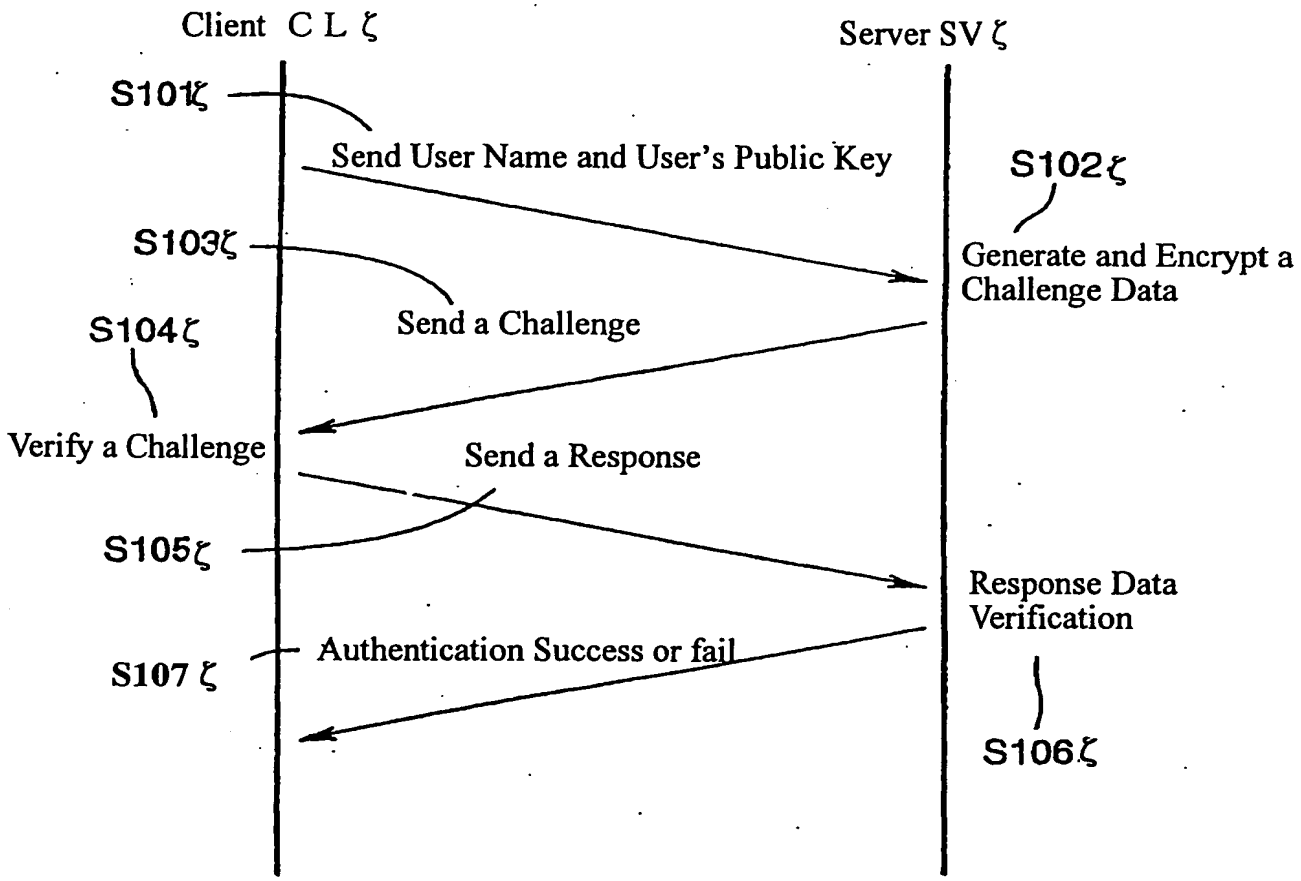
T09020"06E00760

FIG.68



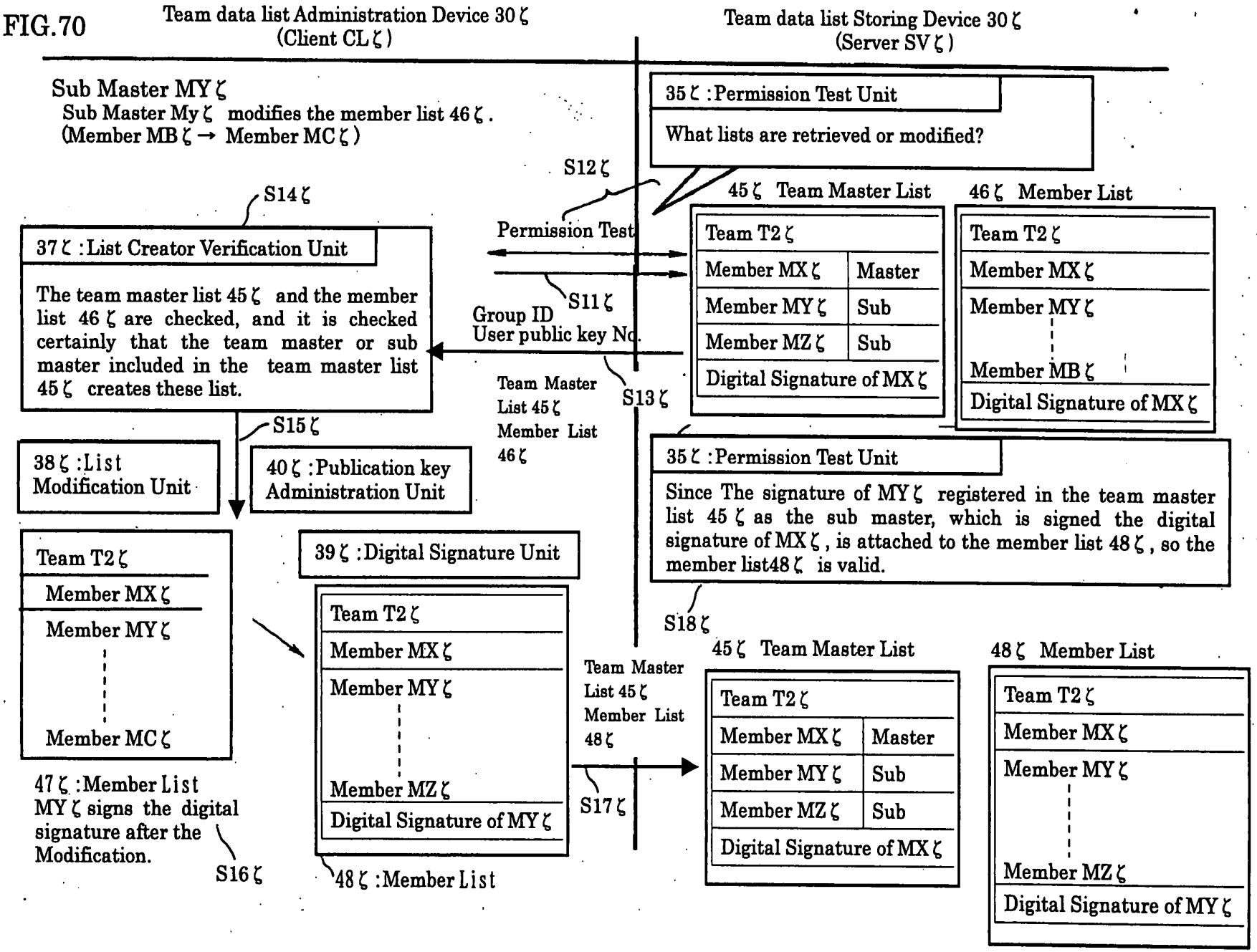
OBLON ET AL (703) 413-3000
DOCKET # 1819.0115/PKS
SHEET 44 OF 77
09/700390

FIG.69


Client C L ζ
Server SV ζ
S101ζ
Send User Name and User's Public Key
S102ζ
S103ζ
Generate and Encrypt a Challenge Data
Send a Challenge
S104ζ
Verify a Challenge
Send a Response
S105ζ
Response Data Verification
Authentication Success or fail
S107 ζ
S106ζ

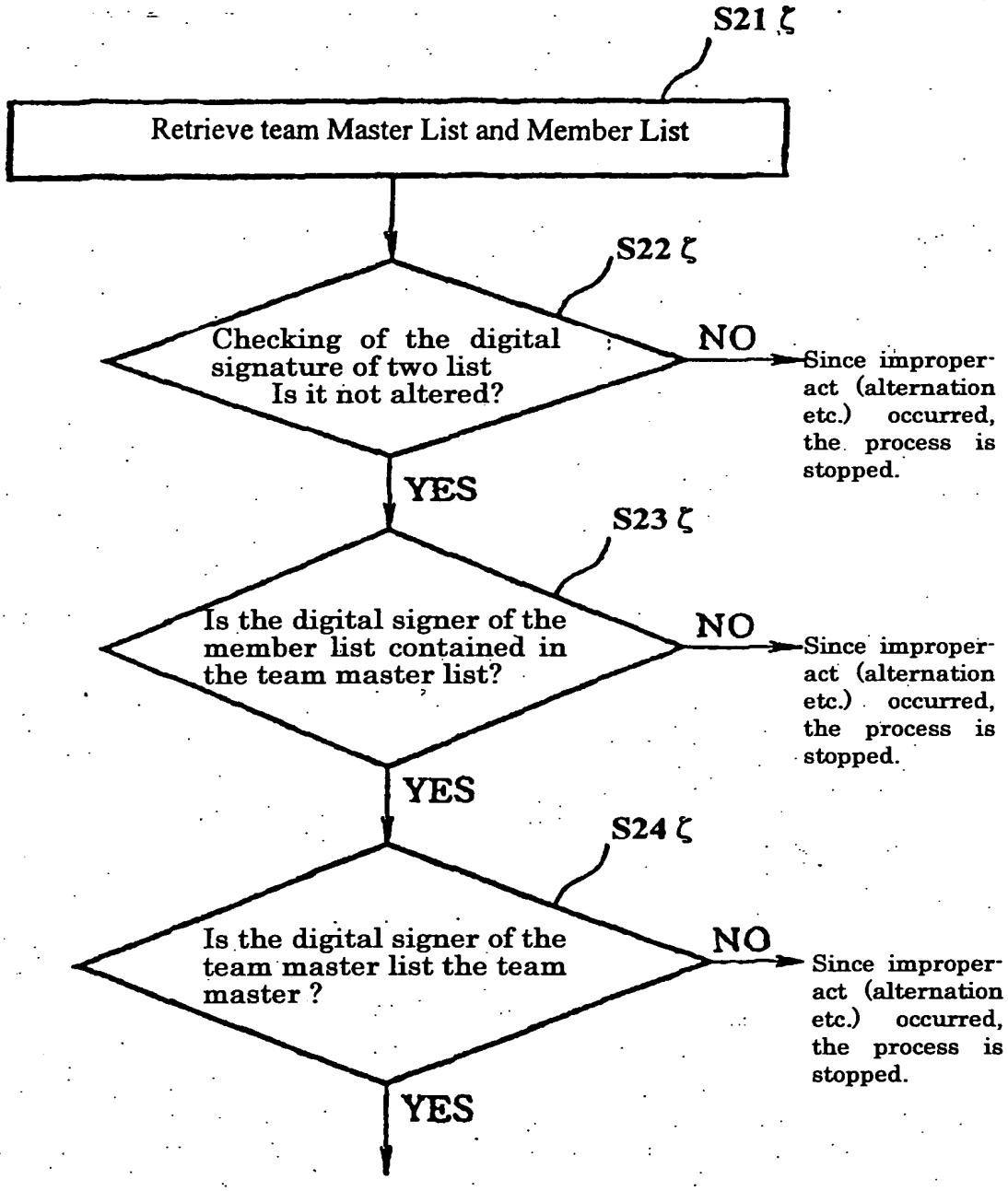
T0902O" 06E00260

FIG.70



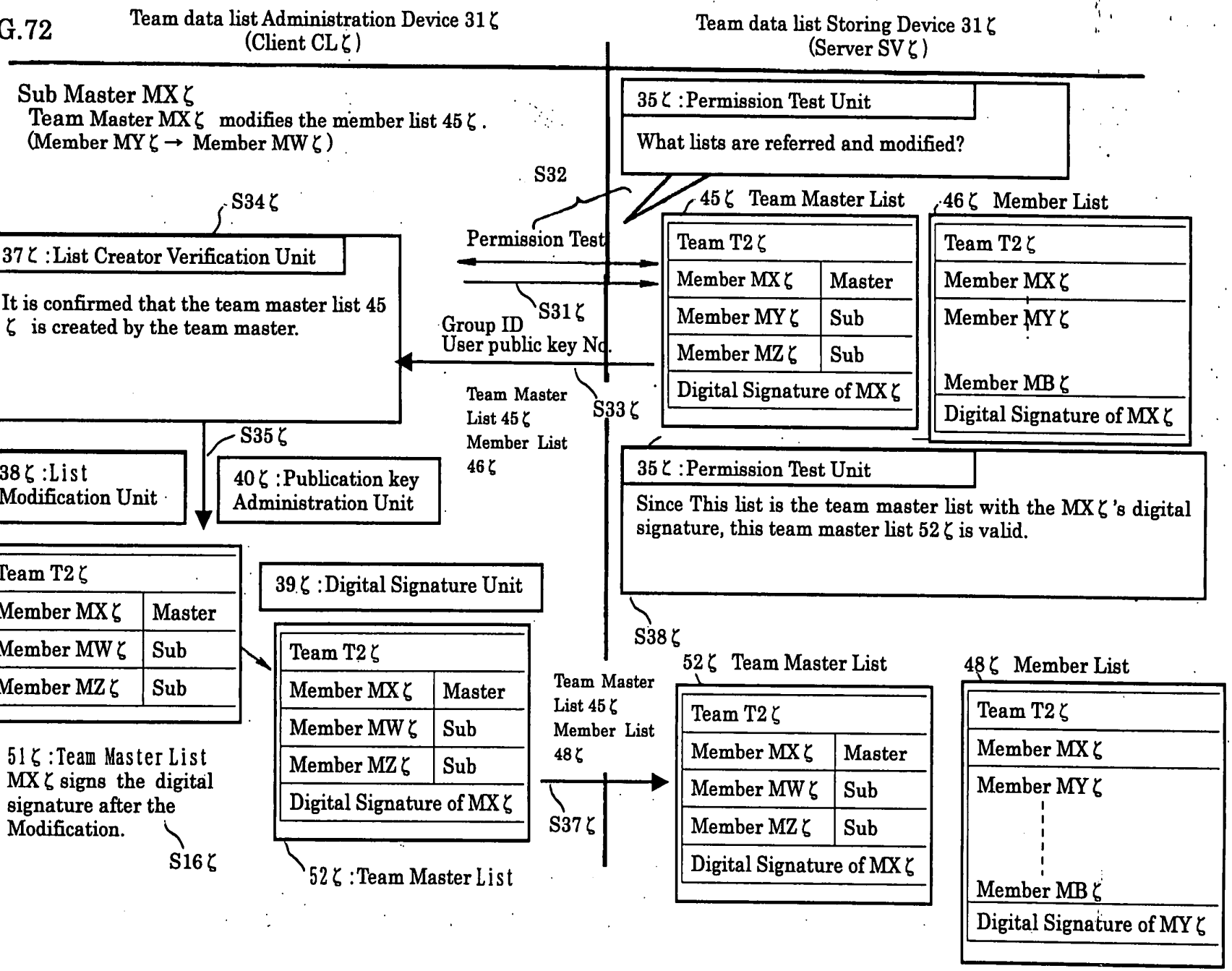
OBLON ET AL (703) 413-3000
DOCKET # 1990US2PCT SHEET 14 OF 19
09/700390

FIG. 71


S21
Retrieve team Master List and Member List
S22
Checking of the digital signature of two list Is it not altered?
NO
Since improper-act (alternation etc.) occurred, the process is stopped.
YES
S23
Is the digital signer of the member list contained in the team master list?
NO
Since improper-act (alternation etc.) occurred, the process is stopped.
YES
S24
Is the digital signer of the team master list the team master ?
NO
Since improper-act (alternation etc.) occurred, the process is stopped.
YES
Since the member list was created by the team master or the sub master with the proper permission, the process is continued.

T09070*06E00760

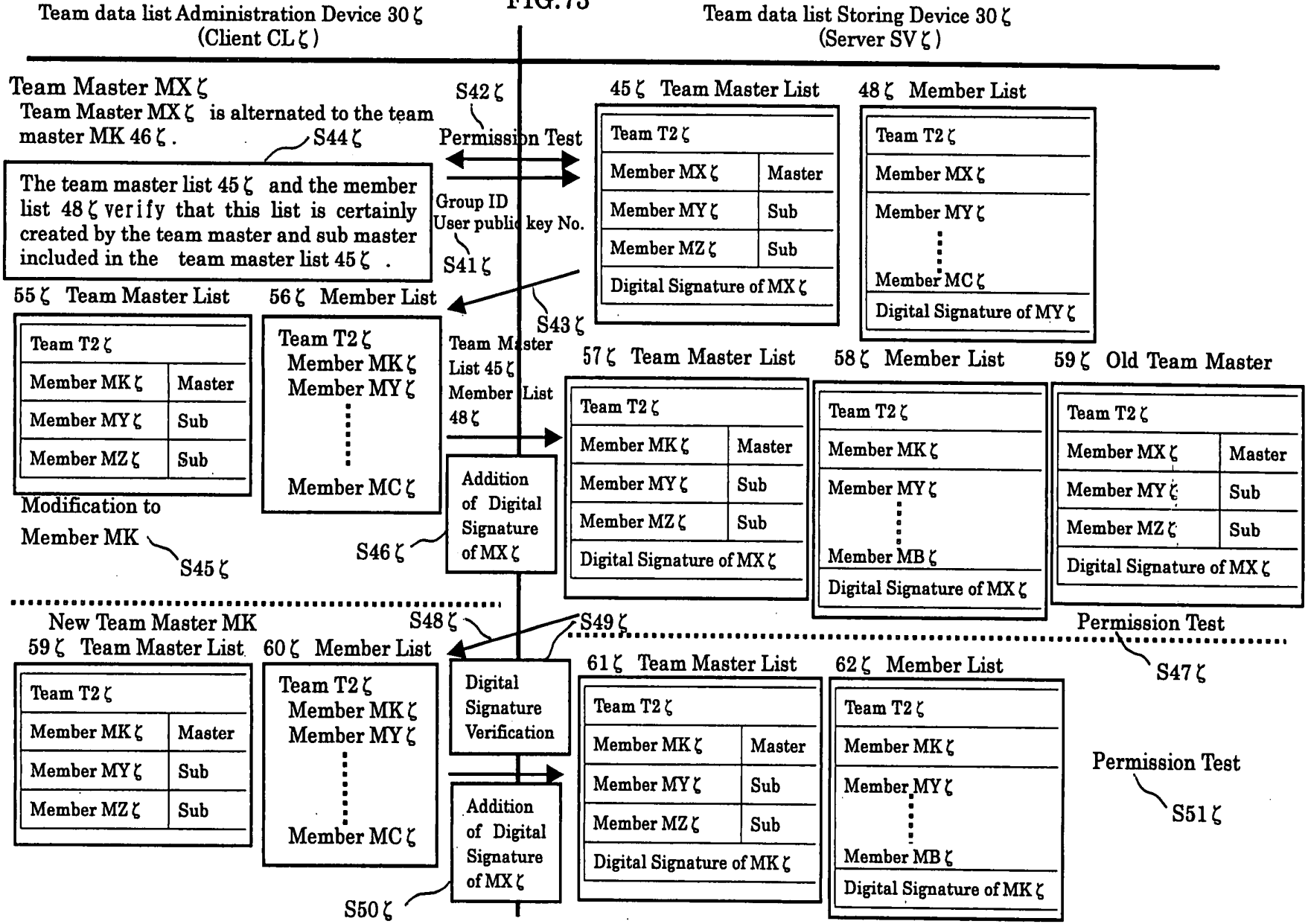
FIG.72



OBLON ET AL (703) 413-3000
DOCKET# 1941.1USP2 SHEET 68 OF 72
09/700390

T09070 "06E00260

FIG.73



OBLON ET AL (703) 413-3000
DOCKET # 1990US02
SHEET 12 OF 13
09/700390

FIG.74

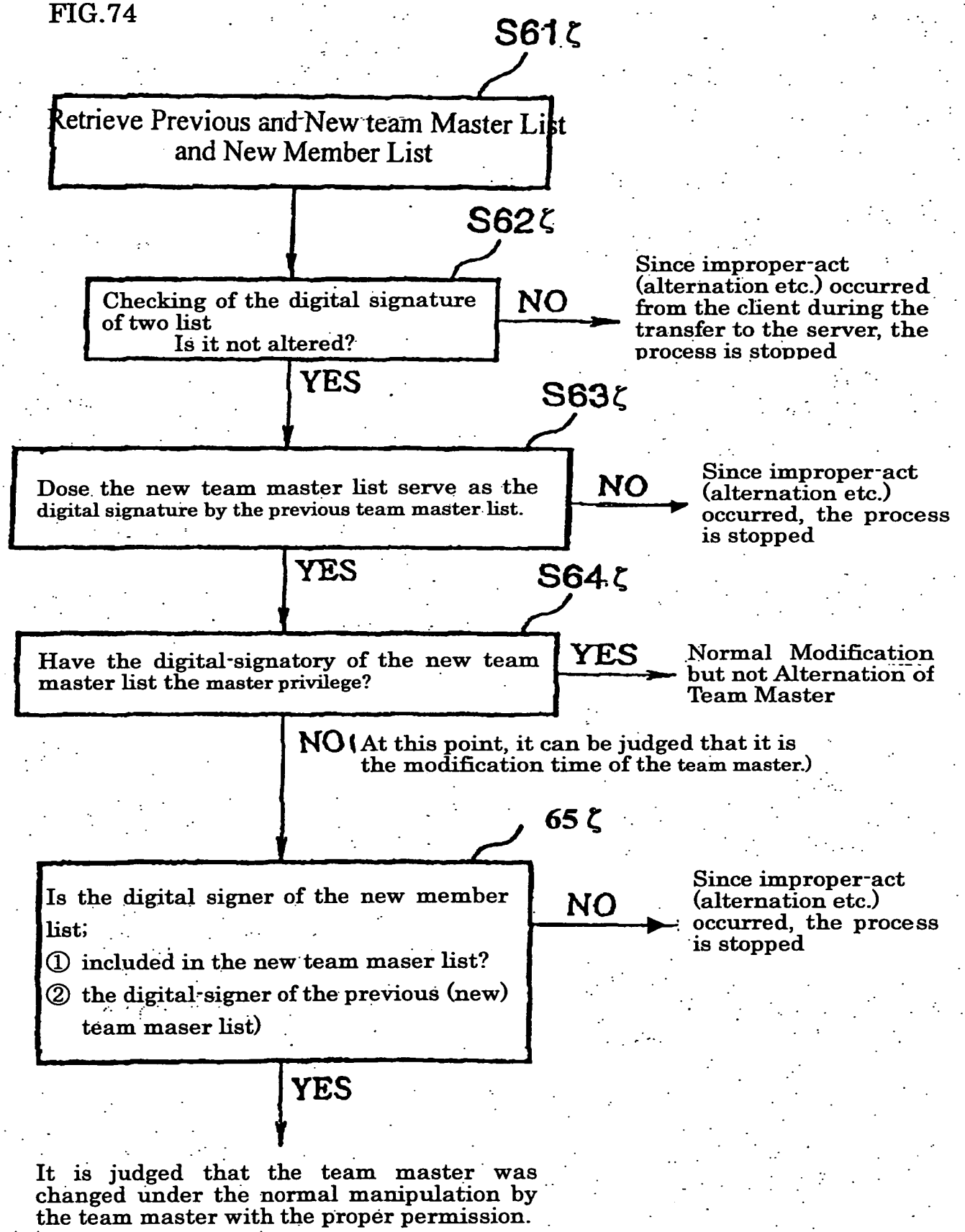
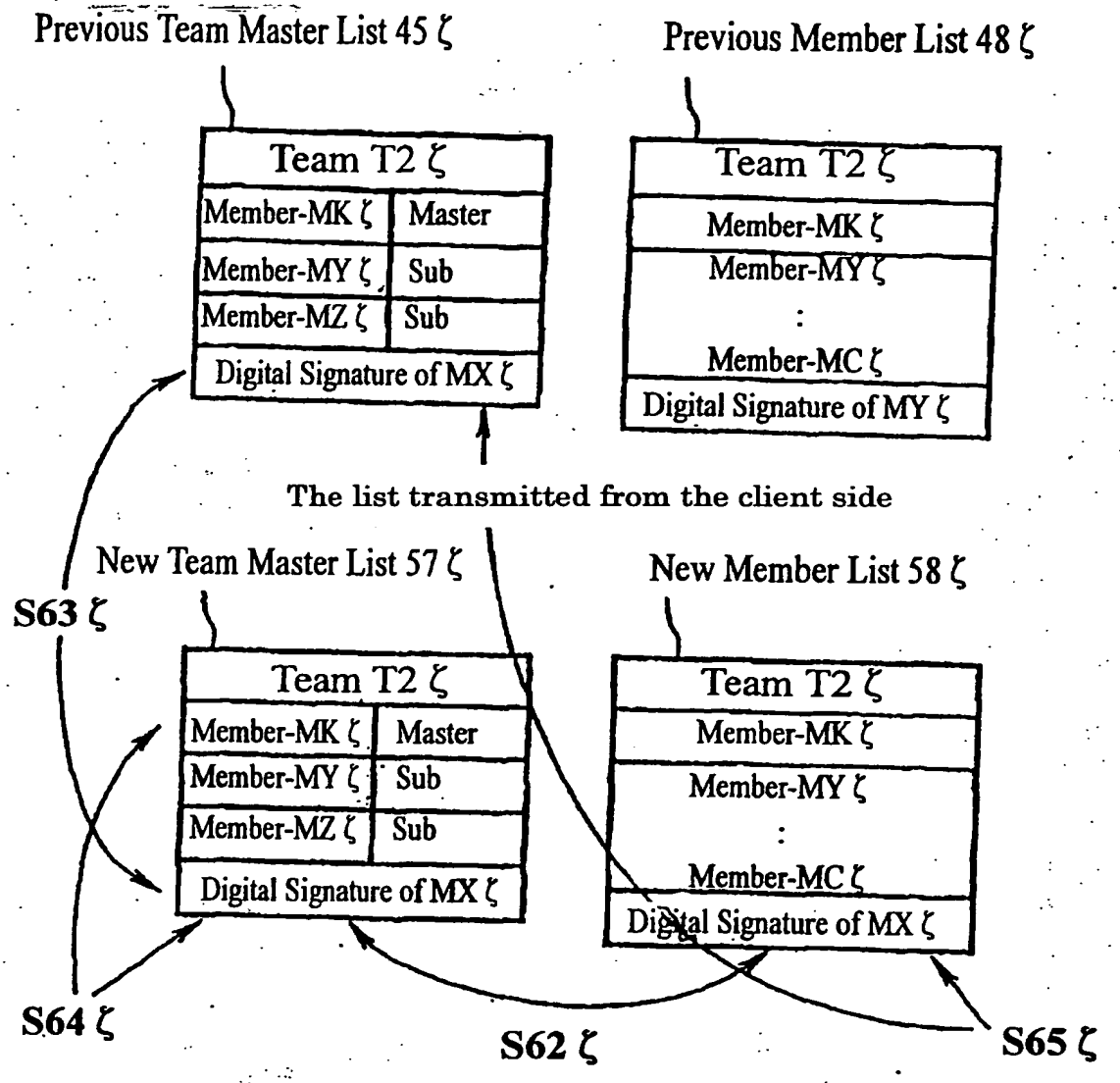

S61
Retrieve Previous and New team Master List and New Member List
S62
Checking of the digital signature of two list Is it not altered?
NO
Since improper-act (alternation etc.) occurred from the client during the transfer to the server, the process is stopped
YES
S63
Dose the new team master list serve as the digital signature by the previous team master list.
NO
Since improper-act (alternation etc.) occurred, the process is stopped
YES
S64
Have the digital-signatory of the new team master list the master privilege?
YES
Normal Modification but not Alternation of Team Master
NO (At this point, it can be judged that it is the modification time of the team master.)
65
Is the digital signer of the new member list;
① included in the new team maser list?
② the digital-signer of the previous (new) team maser list)
NO
Since improper-act (alternation etc.) occurred, the process is stopped
YES
It is judged that the team master was changed under the normal manipulation by the team master with the proper permission.

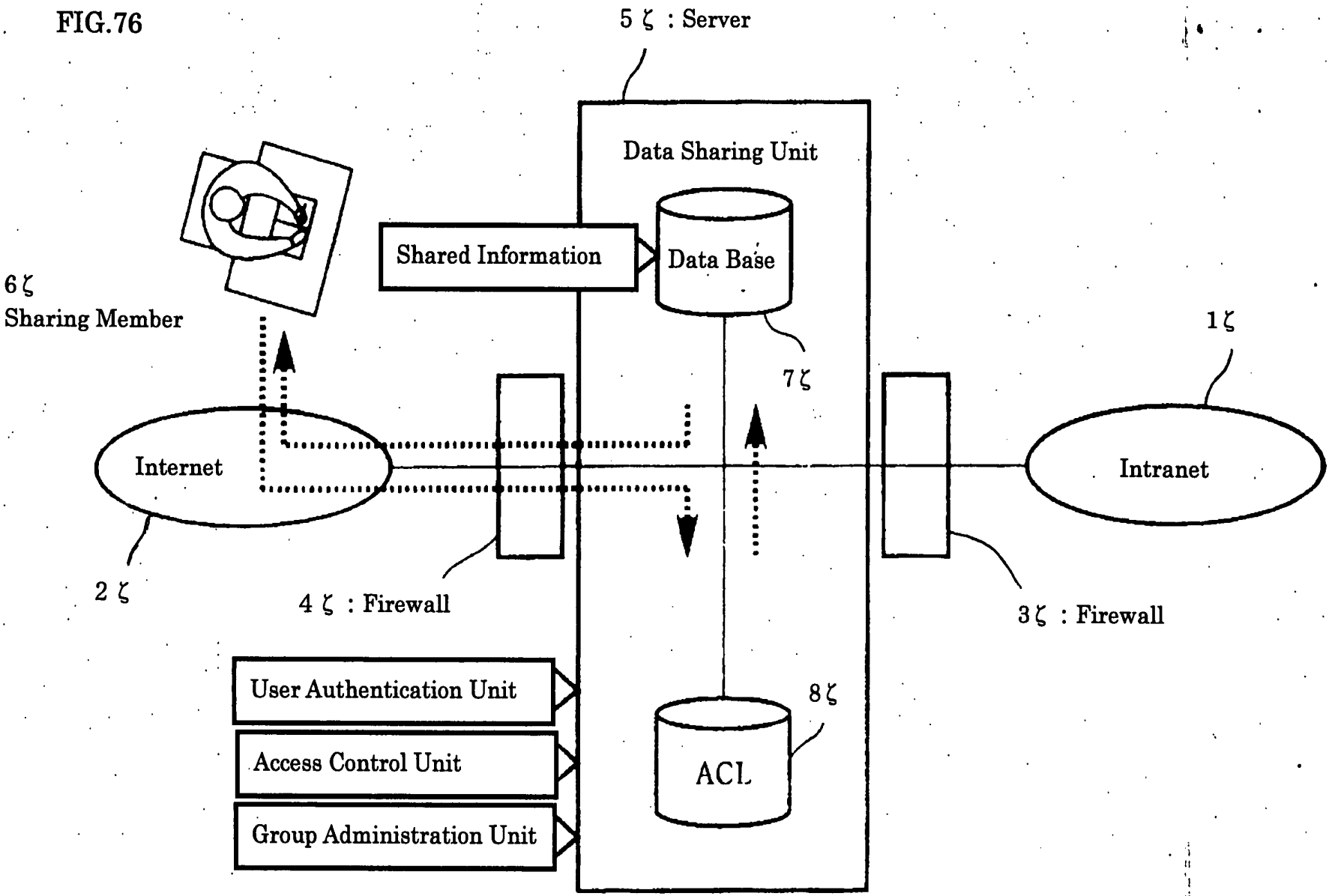
FIG.75

The list stored at the server side



T09020"06E00260

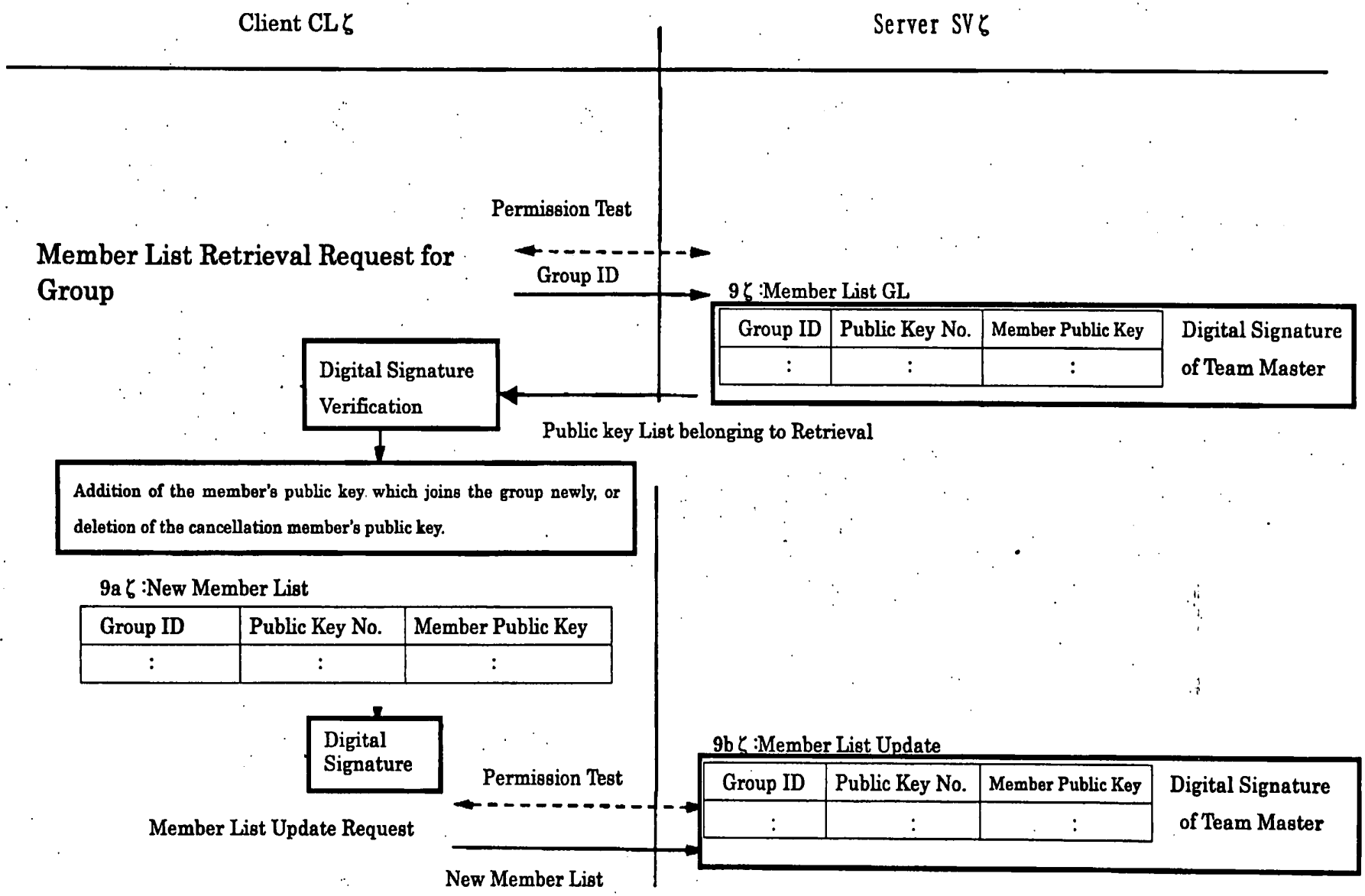
FIG.76



OBLON ET AL (703) 413-3000
DOCKET # 040113-0278
SHEET 12 OF 13
09/700390

T090Z0" 06E00Z60

FIG.77



OBLON ET AL (703) 413-3000
DOCKET # 1410 US01
SHEET 13 OF 18
09/700390